Separable Operations, Graph Codes and the Location of Quantum Information

by

Vlad Gheorghiu

A Dissertation submitted in partial fulfillment
of the requirements for the degree of

Doctor of Philosophy

in the Department of Physics

Carnegie Mellon University
Pittsburgh, Pennsylvania, USA

2010
(Submitted June 1, 2010)

Acknowledgements

I would like to thank to my advisor Robert B. Griffiths for his guidance during my PhD, as well as to the members of the quantum information group at Carnegie Mellon University for useful and stimulating discussions.

Abstract

In the first part of this Dissertation, I study the differences between LOCC (local operations and classical communication) and the more general class of separable operations. I show that the two classes coincide for the case of pure bipartite state input, and derive a set of important consequences. Using similar techniques I also generalize the no-cloning theorem when restricted to separable operations and show that cloning becomes much more restrictive, by providing necessary (and sometimes sufficient) conditions.

In the second part I investigate graph states and graph codes with carrier qudits of arbitrary dimensionality, and extend the notion of stabilizer to any dimension, not necessarily prime. I further study how and where information is located in the various subsets of the qudit carriers of arbitrary additive graph codes, and provide efficient techniques that can be used in deciding what types of information a subset contains.

Contents

List of Tables

List of Figures

1

Introduction and preliminary concepts

1.1 Historical remarks

Classical computers are indispensable in today's world and appear in almost all imaginable scenarios, ranging from simple MP3 players to sophisticated supercomputers used in weather prediction. Although their architecture is strongly device-dependent, they all have one thing in common: every classical computer is a physical realization of a Turing machine, a mathematical model introduced by Alan Turing in 1937 [Tur37] which formalized the concept of computation. Intuitively, any computer with a certain minimum capability is, in principle, capable of performing the same tasks that any other computer can perform, if sufficient time and memory are provided.

The fundamental processing unit of a classical computer is the *bit*: a two-state system commonly denoted by 0 and 1. A computation is performed whenever some input bits are processed by the computer, resulting in another sequence of bits that represent the output of the computation. Any two-state classical physical system can in principle represent a bit, and a classical computer able to operate on these bits and to produce a valid output can (in principle) be built using only classical devices, as billiard balls, pulleys and so on, although in real world applications everything tend to be miniaturized for efficiency purposes.

A fruitful idea is that *computation is physical*: any physical system performs some kind of computation during its evolution. Consider for example a rock that is falling down from some height. The total falling time is directly proportional to the square root of the height, so in a sense by simply measuring the time one effectively computes the square root of the height. With a bit of imagination more sophisticated examples can be constructed. What if we make use of the intimate structure of quantum mechanics and quantum systems to perform computations? Are there any fundamentally new possibilities relative to the classical case, or, is a *quantum computer* potentially more powerful than a classical one? This idea was first introduced in 1982 by Richard Feynman [Fey82], when the notion of a quantum computer was born. One may argue that a rock is also a (quite large) quantum mechanical system, so why should quantum mechanics be more "powerful" in performing computations than its classical counterpart? The main and fundamental difference between classical and quantum mechanics is that the latter has a much richer structure that allows for novel effects not present in classical physics due to its use of a Hilbert space. On larger scales the quantum effects tend to be smoothed out and the system becomes classical, or *decoheres*, but on smaller scales the effects can be quite significant.

Although it was widely believed that a quantum computer can indeed be more powerful than a classical one, in cases such as simulation of complex quantum systems, the first quantum algorithm

able to outperform any known classical version was discovered only in 1994 [Sho97] by the computer scientist Peter Shor. He invented a quantum algorithm able to factor large numbers in polynomial time and that did not (and still does not) have any efficient classical counterpart.

Even though a genuinely good quantum algorithm existed, a great deal of skepticism was displayed with respect to an actual physical realization. It was already known that quantum systems are very sensitive to external noise that induce *errors* in the computation, and the main problem seemed to be the inability to correct these errors. Classical error correction was well understood [MS77], the basic idea behind the whole field being the usage of *redundancy*, or duplication of information for better protection against errors. On the other hand, the "no-cloning" theorem of Wootters and Zurek [WZ82], discovered in 1982, forbids the duplication of quantum information, e.g. non-orthogonal states cannot be duplicated. Therefore the perspectives for good *quantum error correction* schemes looked extremely unpromising. The solution was provided by the same Peter Shor in 1995 [Sho95], who showed that good quantum error correction schemes, which are not simply based on duplication of quantum information, exist. Quantum error correcting codes are of extreme importance in quantum information processing since they allow for high-fidelity transmission of quantum information and reduction of decoherence.

A novel field of science, Quantum Computation and Quantum Information, suddenly became a hot topic at the intersection of physics, mathematics and computer science. It has developed rapidly since 1994 and remarkable theoretical as well as experimental progress has been achieved. Today the subject is still far from being well understood, and I hope this Dissertation contains some nontrivial contributions to it.

1.2 Preliminary concepts

1.2.1 Qubits and qudits

The fundamental processing unit of a quantum computer is the *qubit*: a quantum system with two energy levels. The state of the qubit is often denoted by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

where α and β are complex coefficients satisfying $|\alpha|^2 + |\beta|^2 = 1$ and $|0\rangle$ and $|1\rangle$ are orthonormal basis vectors of a 2-dimensional complex Hilbert space $\mathcal{H}$. The *qudit* is the natural generalization of the qubit to D level quantum systems and is represented by a complex Hilbert space of dimension D.

1.2.2 Evolution and quantum channels

The evolution of a quantum system interacting with an external environment is in general non-unitary. A standard way of describing such evolution uses the Kraus formalism: if the initial state of the system is given in terms of a density operator ρ, then after a time t the state evolves as

$$\rho \to \sum_k F_k \rho F_k^\dagger, \tag{1.2}$$

where the F_k are called *Kraus operators* that satisfy the *closure condition*

$$\sum_k F_k^\dagger F_k = I, \tag{1.3}$$

where I denotes the identity operator. The Kraus representation (1.2) can be formally derived by considering a unitary evolution of the combined system-environment, and then tracing away (or

measuring) the environment degrees of freedom. A non-trivial result is that any open quantum evolution can be represented in the form (1.2). If the result of the measurement on the environment is known, e.g. equals k, then conditioned on this k the initial density operator of the system is transformed to

$$\rho \to \frac{F_k \rho F_k^\dagger}{\mathrm{Tr}[F_k \rho F_k^\dagger]}. \tag{1.4}$$

However, measurement is not a deterministic operation and the result k is obtained with some probability $p_k = \mathrm{Tr}[F_k \rho F_k^\dagger]$. Therefore whenever the measurement results on the environment are not discarded, the initial density operator of the system is transformed to an *ensemble*

$$\rho \to \{p_k, \rho_k\}, \quad \rho_k = \frac{F_k \rho F_k^\dagger}{\mathrm{Tr}[F_k \rho F_k^\dagger]}. \tag{1.5}$$

If the system starts out in a pure state $|\psi\rangle$, then (1.5) reduces to

$$|\psi\rangle \to \{p_k, |\psi_k\rangle\}, \text{ with } F_k|\psi\rangle = \sqrt{p_k}|\psi_k\rangle \text{ and } p_k = \langle\psi|F_k^\dagger F_k|\psi\rangle. \tag{1.6}$$

Any evolution of the form (1.2) is also called a *quantum channel*, and (1.2) represents the Kraus representation of a quantum channel. Technically the map (1.2) is a completely positive trace preserving (CPTP) map, which intuitively means that it maps positive operators to positive operators, remains positive whenever the system is trivially enlarged to a larger one, and preserves the trace of an operator. The latter condition is imposed by the closure condition (1.3) and ensures that probability is conserved. The study of quantum channels is the subject of intense theoretical investigations as they are much less understood than their classical counterpart. The interested reader can consult Chapter 8 of [NC00] for a good introduction to the subject.

1.2.3 Bipartite (multipartite) quantum systems

In quantum theory a multipartite quantum system is described by a Hilbert space constructed as a tensor product of the individual Hilbert spaces, and any vector in this tensor product space represents a valid quantum state. This is one instance in which quantum mechanics has a much richer structure than classical mechanics, because the tensor product description allows the existence of *entangled states*, i.e. quantum states that cannot be written as a tensor product of individual states. For example, in a bipartite qubit quantum system represented by a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, a state of the form

$$|\psi\rangle = \alpha|00\rangle_{AB} + \beta|11\rangle_{AB} \tag{1.7}$$

with $|\alpha|^2 + |\beta|^2 = 1$ is entangled as long as $0 < |\alpha|^2 < 1$. Otherwise it is called a *product state*. Whenever $|\alpha| = |\beta| = 1/\sqrt{2}$ the state is called *maximally entangled*. Throughout this Dissertation I will use the shorthand notation $|00\rangle_{AB}$ to denote the tensor product $|0\rangle_A \otimes |0\rangle_B$.

It turns out that any normalized bipartite entangled state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written in a canonical form known as the *Schmidt form*: there always exist orthonormal bases $\{|a_j\rangle\}$ and $\{|b_k\rangle\}$ of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, in which the $|\psi\rangle$ has the form

$$|\psi\rangle = \sum_{r=0}^{D-1} \sqrt{\lambda_r}|a_r\rangle_A|b_r\rangle_B. \tag{1.8}$$

Here D is the minimum of the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$. The λ_r's can always be chosen to be positive real numbers that satisfy $\sum_r \lambda_r = 1$ and are called *Schmidt coefficients*. An alternative definition is that a bipartite pure state is maximally entangled if and only if all Schmidt coefficients are equal. When all Schmidt coefficients except one are zero then the state is a product state,

otherwise it is partially entangled. The number of positive Schmidt coefficients is called the *Schmidt rank* of $|\psi\rangle$. If all Schmidt coefficients are strictly positive than we say that $|\psi\rangle$ has *full Schmidt rank*. There is no analog of the Schmidt form for multipartite pure states, and this constitutes a major obstacle in understanding them.

Entanglement is often considered a precious resource, since it can be "consumed" by various non-classical protocols such as quantum teleportation [BBC+93], quantum dense coding [BW92] etc. It also constitutes a key ingredient (although by no means the only one) in the construction of good quantum error codes and exponentially faster quantum algorithms, and therefore its study constitutes an important part of quantum information theory.

1.2.4 LOCC and Separable Operations

An important paradigm in quantum information is that of local operations and classical communication (LOCC). Consider for example two spatially separated parties, traditionally named Alice and Bob, each having access to local quantum systems described by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Both Alice and Bob are allowed to perform arbitrary quantum operations on their individual quantum systems, and can also make use of a classical channel to communicate. They are not allowed, however, to exchange quantum systems between themselves nor to use a quantum channel. What kind of tasks can be performed in this paradigm? What are the restrictions compared to the global case (i.e. when global quantum operations are allowed on the combined system $\mathcal{H}_A \otimes \mathcal{H}_B$)? Understanding LOCC constitutes an extremely important research program, since in an actual realization of a quantum computer many qubits may be well separated in space, and performing a global operation on them, in contrast to LOCC, will often be challenging, at least from an experimental point of view.

Every LOCC operation can be regarded as a composition of local operations conditioned on particular measurement results that may be communicated through the classical channel. It is not hard to see that the initial state ρ of a quantum system transforms under LOCC as

$$\rho \to \sum_k (A_k \otimes B_k)\rho(A_k \otimes B_k)^\dagger, \tag{1.9}$$

with

$$\sum_k (A_k^\dagger A_k \otimes B_k^\dagger B_k) = I_A \otimes I_B. \tag{1.10}$$

The concepts above generalize to more than two parties in a straightforward manner.

One may be tempted to say that any quantum operation of the form (1.9) represents a valid LOCC, but this is not true! There are operations of this form that are not LOCC [BDF+99], that is, cannot be implemented by an LOCC paradigm, and which are called *separable operations*. There exists a simple example [BDF+99] of a set of basis states in a bipartite qutrit ($D = 3$) system that cannot be distinguished by LOCC but can be distinguished by separable operations. Hence LOCC is a proper subset of this more general class of separable operations. Although separable operations are not always implementable by LOCC, studying them is worthwhile since in general they have a cleaner mathematical formulation than LOCC and any result proven to be true for all separable operations will automatically be valid for LOCC, since the latter is a subset of the former.

In the bipartite setting, a maximally entangled state plays the role of a universal resource, i.e. from an operational point of view can be transformed deterministically by LOCC to any bipartite partially entangled state [Nie99]. This is not true anymore in the multipartite regime; there is no universal multipartite quantum state that can be transformed to any arbitrary multipartite state by LOCC [HHHH09].

Entanglement can be quantified by various measures, and the measure is called an *entanglement monotone* if it is non-increasing under LOCC. In general entanglement measures have a simple form only for pure bipartite states, and in this case depend only on the Schmidt coefficients of the state.

For multipartite pure states or even for bipartite mixed states such a Schmidt decomposition does not exist, and entanglement in these cases is far from being understood. For a good introduction to the theory of entanglement see [HHHH09].

1.2.5 Graph states and graph codes

Quantum states and quantum entanglement are much better understood in the bipartite setting than in the multipartite setting. Two main difficulties that arise in the latter case are: i) the exponential growth, with the number of constituent parts, of the number of complex amplitudes used to describe a multipartite quantum state, and ii) the non-existence of a Schmidt representation.

However, *graph states* form a class of multipartite states with a fairly simple structure. Given a graph $G = (V, E)$ with n vertices V, each corresponding to a qubit, and a collection E of undirected edges connecting pairs of distinct vertices (no self loops are allowed), a graph state is obtained by preparing a set of initial qubits in the $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ state, then applying controlled-phase gates between any two neighbors that are connected by an edge in the corresponding graph. Graph states can be generalized to higher dimensional qudits in a direct manner, using graphs with multiple edges, as described in detail in Chapters 5 and 6.

Graph states were first introduced by Raussendorf and Briegel [RB01] in their *measurement-based computation model*(often called the *one-way model*). This new model of quantum computation is fundamentally different from the well-known circuit model, and is also universal. Any desired quantum computation can be achieved by only performing local measurements (in a basis that is conditioned on previous measurement results) on the qubits of a sufficiently large cluster state, a graph state in which the graph is a finite part of a lattice such as the square lattice. Graph states are therefore universal resources for quantum computation and intense theoretical as well as experimental work has been dedicated to their study. For a comprehensive introduction to the subject see [HDE$^+$].

Graph states are also an instance of the so-called *stabilizer states* [Gotb]. A stabilizer state is a multipartite quantum state that can be described by an Abelian group (the stabilizer group) of Pauli-like operators on the Hilbert space of the carriers, each of which leaves the state invariant. Instead of describing a stabilizer state of n qubits by 2^n complex amplitudes, it is enough to specify the generators of its stabilizer group of which there are no more than n. Hence stabilizer states allow for a very compact description. Stabilizer states play an extremely important role in the theory of quantum error-correction codes and they extend the notion of linear classical error correcting codes [MS77] to the quantum domain.

1.2.6 Location of information

First let us define what we mean by (classical) information. Information is embedded in correlations between two systems, e.g. we say that information about a system A is "located" in another system B if the statistical correlations between A and B are such that information about some properties of A can be recovered from B. For example, the photons that bounce off the Sunday newspaper hit the reader's retina and correlations between the letters on the newspaper page and reader's brain are established: the information about the latest news is now located in the reader's brain. If the systems are perfectly correlated then we say that all information about A is perfectly present in B, and if they are totally uncorrelated than we say that no information about A is present in B (or, equivalently, that all information about A is absent from B). Traditionally A is considered to be the input of a communication channel and B its output at a later time, but information theory is not restricted to channels.

Whereas the concept seems to be quite natural and simple, the rigorous mathematical theory of information was founded by Claude Shannon only in 1948 [Sha48] and has been continuously developed since then (see [CT05] for a comprehensive introduction). Information theory is a very

important subject in modern communication, cryptography, classical error-correcting codes etc, with applications ranging from audio CD error-correction to military satellite communication.

Unlike classical information, quantum information can be present in more than one "type", a terminology introduced by Griffiths [Gri07], and various types can be incompatible, e.g. associated to operators that do not commute. Formally, a type of information is associated with a projective decomposition of the identity

$$I = \sum_j P_j, \quad P_j = P_j^\dagger = P_j^2. \tag{1.11}$$

We also associate a type of information with a normal operator through its spectral decomposition, and, for example, call the information corresponding to the x component of an angular momentum of a spin one-half particle, represented by the Pauli operator σ_x, usually denoted by X, the X-type of information, and the information corresponding to the z component as the Z-type of information. Of course the X and Z types are incompatible, since their corresponding operators do not commute.

1.3 Overview of the Dissertation

1.3.1 Separable operations

An LOCC acting on a pure bipartite state $|\psi\rangle_{AB}$ will in general produce an ensemble of states $\{p_k, |\phi_k\rangle_{AB}\}$, where p_k is the probability of obtaining the result k through a measurement of the environment. Finding necessary and sufficient conditions for when such a transformation is possible represents an important problem, and a complete solution for bipartite systems was first provided by Nielsen for an ensemble with only one output state [Nie99] and generalized by Jonathan and Plenio to ensembles with a finite number of states [JP99]. Both of these necessary and sufficient conditions are given in terms of *majorization relations* [Bha97] between Schmidt coefficients, and they completely characterize LOCC operations acting on pure bipartite states.

In Chapter 2 and Chapter 3 we study separable operations acting on a pure bipartite state, trying to generalize previously known results. The most important result is that any output ensemble produced by a separable operation acting on a pure bipartite state can in fact be produced by some LOCC acting on the same state. Our result effectively says that LOCC and separable operations are the same class of quantum operations when acting on pure bipartite states. In particular, we prove that the majorization conditions of Jonathan and Plenio [JP99] are necessary and sufficient in the more general case of separable operations.

Our result also has important consequences in the theory of entanglement, implying that a large number of mixed-state entanglement monotones remain monotone under separable operations. Since such monotonicity under LOCC has long been considered a necessary, or at least a very desirable condition for any "reasonable" entanglement monotone, one wonders whether monotonicity under separable operations, in principle a stronger condition, might be an equally good or even superior desideratum.

An interesting question that follows from our result is: are separable operations and LOCC the same class of quantum operations when acting on multipartite pure states? It might be, but proving it would require very different methods than the ones we used, since there are no simple analogs of the Schmidt decomposition and majorization conditions. Necessary and sufficient conditions are not known even for LOCC.

1.3.2 Local cloning of bipartite entangled states

In Chapter 4 we consider the slightly different problem of cloning orthogonal entangled states by separable operations, a problem that belongs to the more general framework of deterministic mapping of an ensemble of pure states (and not just one state, as before) into another ensemble of pure states

by a separable operation. As summarized by the "no-cloning" theorem of [WZ82], any set of quantum states can be deterministically cloned if and only if the states in the set are mutually orthogonal. When the states are not orthogonal, there is no deterministic apparatus capable of performing such a cloning. However, probabilistic cloning may still be possible and a significant amount of work has been dedicated to studying this case [SIGA05].

Formally, a set of quantum states $\{|\psi_j\rangle\}$ is cloned whenever there exist a quantum operation that performs

$$|\psi_j\rangle \otimes |\phi\rangle \to |\psi_j\rangle \otimes |\psi_j\rangle, \quad \forall j. \tag{1.12}$$

If the transformation is deterministic for all j, then the cloning is deterministic. Otherwise is probabilistic. The state $|\phi\rangle$ plays the role of a resource or a "blank state" in which the copy of $|\psi_j\rangle$ is to be imprinted.

When the set consists of bipartite entangled states, and the cloning is restricted to LOCC (or to separable operations), the problem becomes much more difficult, and further restrictions have to be imposed. The mere orthogonality of the states no longer implies that they can be (locally) cloned. An LOCC analog of the "no-cloning" theorem was not yet found, and finding it may prove useful.

It turns out that any two (and no more than two) orthogonal maximally entangled two-qubit states can be locally cloned by LOCC, using a maximally entangled "blank state" [ACP04] (on which the copy is to be imprinted). A generalization to D maximally entangled states of two qudits of prime dimension D was given in [OH06], which showed that a set of D such states can be locally cloned using a maximally entangled resource if and only if the states in the set are locally (cyclically) shifted

$$|\psi_i\rangle = \frac{1}{\sqrt{D}} \sum_{r=0}^{D-1} |r\rangle^A |r \oplus i\rangle^B, \tag{1.13}$$

where the $\oplus$ symbol denotes addition modulo D. Kay and Ericsson [KE06] extended the above results to the LOCC cloning of full Schmidt rank partially entangled states using a maximally entangled blank state. They presented an explicit protocol for the local cloning of a set of $D \times D$ cyclically shifted partially entangled states of the form

$$|\psi_i\rangle = \sum_{r=0}^{D-1} \sqrt{\lambda_r} |r\rangle^A |r \oplus i\rangle^B \tag{1.14}$$

using a maximally entangled blank state, but failed to prove that any clonable set of states must be of this form.

We investigate the conditions under which a set of pure bipartite quantum states on a $D \times D$ system can be locally cloned deterministically by separable operations when at least one of the states is full Schmidt rank. We do not assume that D is necessarily a prime number and we also allow for the possibility of cloning using a resource state that is less than maximally entangled. We derive a set of necessary conditions, that are also sufficient in the case of qubits. In this latter case we proved a long-standing conjecture that a maximally entangled state is a necessary resource for such local cloning, even if the states to be cloned are partially entangled. We also generalize the protocol of Kay and Ericsson and show that any set of partially entangled "group-shifted" states

$$|\psi_f\rangle = \sum_{g \in G} \sqrt{\lambda_g} |g\rangle^A |fg\rangle^B, \tag{1.15}$$

where G is a group of order D and the elements of the group label an orthonormal basis of the (local) Hilbert space, can be locally cloned using a maximally entangled blank state, by providing an explicit LOCC circuit. Our protocol reduces to the one of Kay and Ericsson in the case of cyclic groups, since the latter is isomorphic to the additive group of integers mod D and the set of states defined by (1.14) and (1.15) are the same.

Our results significantly extend previous work in the literature (limited only to LOCC) [GKR04, ACP04, OH06, KE06, CKRR07].

1.3.3 Graph codes

Using graph states provides a fruitful approach for constructing good quantum error correcting codes, called *graph codes*. A graph code is a subspace of the Hilbert space of n carrier qubits spanned by a collection of *graph basis states*: a quantum state obtained from a fixed graph state by applying local Z operators on some of the qubits. See Chapter 5 for a detailed introduction to graph codes.

There have been extensions to higher dimensional qudits, but all of them considered only qudits of prime dimensionality D. The main difficulty in the non-prime case is that $\mathbb{Z}_D$ is a ring, not a finite field, and the lack of the multiplicative inverse operation poses some technical problems, which we have successfully solved.

Most known quantum error correcting codes are graph codes or are equivalent to graph codes under local unitary transformations, hence understanding them is extremely important. In Chapter 5 we present an elegant method for constructing such graph codes, allowing for carrier qudits of arbitrary dimensionality, not necessarily prime. Our method allows for *additive* (or stabilizer [Gotb]) as well as non-additive graph codes and was simultaneously developed by Cross et al [CSSZ09] for qubits and Chen et al [CZC08] for higher dimensional qudits. We use simple graphical methods and computer searches to construct both additive and non-additive quantum error correcting codes, but computer searches are much faster for additive codes. In a number of cases we have been able to construct what we call quantum Singleton codes that saturate the quantum Singleton bound [KL97]. Our numerical techniques are based on finding a *maximum clique* [GJ79] in some related graph. The maximum clique problem on a general graph is known to be NP-complete, but our method may still be useful for constructing quantum codes with relatively small number of carriers. We also generalize the concept of a stabilizer group to the non-prime case and derive an elegant duality (known before only in the prime case) between the coding space and its corresponding stabilizer group.

1.3.4 Location of quantum information

In Chapter 6 we develop a mathematical formalism that can be successfully applied in studying how quantum information is encoded in additive graph codes and where is it located, a subject closely related to the one of Chapter 5. Studying additive graph codes is worthwhile since the vast majority of quantum error correcting codes are stabilizer codes, and stabilizer codes are locally equivalent to additive graph codes [Schb].

We show how to encode some input quantum information in the *carrier* qudits of an additive graph code and demonstrate how to use the concept of types of information to study the location of quantum information in arbitrary subsets of the carrier qudits. What types and how much information about the input can be then recovered? To various types of information we associate a collection of operators on the coding space which form what we call the information group. It represents the input information through an encoding operation constructed as an explicit quantum circuit (hence generalizing the encoding methods developed before only for prime dimensional qudits). Our formalism is very general and works for arbitrary additive graph codes of arbitrary dimension (not necessarily prime). We also present an efficient numerical algorithm that can be successfully used in deciding where information is located and which types of information are present. As a side remark, note that we have not studied the "recovery problem", i.e. finding the decoding operation that effectively "extracts" the quantum information from some carrier qudits, but in principle such a decoding always exist, provided all quantum information is located in these qudits. This recovery operation is interesting, but is not included in this Dissertation.

The methods presented here allow for a better understanding of the intimate nature of quantum codes and may be of use in constructing better quantum error-correcting codes or quantum secret sharing schemes [MS08].

1.3.5 Bipartite equientangled bases

Chapter 7 is not closely related to the other chapters but presents a solution to a problem posed in [KM06] of constructing a family of "equientangled bases" for a bipartite system of two qudits of arbitrary (but equal) dimension: (i) The basis continuously changes from a product basis to a maximally entangled basis, by varying a parameter t, and (ii) for a fixed t, all basis states are equally entangled.

We actually construct two solutions to the problem, one based on quadratic Gauss sums and the other using qudit graph states. These bases may find applications in various quantum information protocols including quantum cryptography, optimal Bell tests, investigation of the enhancement of channel capacity due to entanglement and the study of multipartite entanglement.

1.4 The structure of the Dissertation

All chapters of this Dissertation are self contained and consist of published (or accepted for publication) articles in refereed journals. The contents of each chapter is almost the same as that of the published paper, with minor modifications made for the sake of consistency of notation throughout the Dissertation. Most of the chapters represent collaborative work with different persons in our research group, as described below.

- Chapter 2, **Entanglement transformations using separable operations**: published in Physical Review A [GG07]. Collaboration with Robert B. Griffiths. Both authors made major contributions. My most important contributions were: i) the application of map-state duality formalism ii) the idea of using an inequality by Minkowski in deriving necessary conditions for pure state transformations under separable operations, and iii) the investigation of random separable unitary channels.

- Chapter 3, **Separable operations on pure states**: published in Physical Review A as a Rapid Communication [GG08]. Collaboration with Robert B. Griffiths. Both authors made major contributions. My most important contributions consisted in: i) extensive numerical studies that led us to the conjecture that separable operations are implementable by LOCC in the case of pure bipartite states; ii) the application of map-state duality formalism; iii) parts of the proof of the main majorization theorem that was conjectured by Griffiths; iv) derivation of the consequences of our result, the most important being that all convex-roof mixed state entanglement measures remain monotone under the more general class of separable operations.

- Chapter 4, **Local cloning of entangled states by separable operations**: accepted for publication in Physical Review A and available on arXiv [GYC]. Collaboration with Scott M. Cohen and Li Yu. I made major contributions to this work, including: i) the map-state duality formalism used in our investigation of the problem; ii) various necessary conditions, such as the necessary form of qubit entangled states, equality of G-concurrence, information-theoretical observation etc.; and iii) various proofs of theorems. Scott Cohen introduced the idea of using finite groups to study sets of clonable states, and Li Yu proved that a maximally entangled state is necessary for the local cloning of group shifted states in $D = 2$ and $D = 3$.

- Chapter 5, **Quantum error correcting codes using qudit graph states**: published in Physical Review A [LYGG08]. Collaboration with Shiang Yong Looi, Li Yu and Robert B. Griffiths. This work was not one of my main projects. My main contributions consisted in developing the stabilizer formalism for non-prime qudits in Sec. 5.5, and proof of the $X - Z$ rule for qudit graph states in Sec. 5.A. I was not involved in the numerical work for searching good quantum error-correcting codes.

- Chapter 6, **Location of quantum information in additive graph codes**: published in Physical Review A [GLG10]. Collaboration with Shiang Yong Looi and Robert B. Griffiths. I had a major part in this paper, together with my co-authors. My most important contributions were: i) introducing a set of useful Clifford gates for arbitrary dimensions; ii) the use of Smith diagonal forms over rings of integers, which allows one to deal with problems that appear in the non-prime case; iii) the discovery of a general encoding operation in terms of an explicit quantum circuit that extended previous work restricted to qudits with prime D; iv) implementation of an efficient linear-algebra algorithm used to decide where and which types of informations are present in a given subset of the carriers; v) proofs of various theorems.

- Chapter 7, **Bipartite equientangled bases**: accepted for publication in Physical Review A and available on arXiv [GL]. Collaboration with Shiang Yong Looi. This work was split into two parts, between myself and my co-author. I found the solution based on Gauss sums (first part), whereas my co-author found the one based on graph states (second part). I also studied the entanglement properties of the second solution in terms of G-concurrence, and proved its monotonicity as a function of t.

2

Entanglement transformations using separable operations

2.1 Introduction

A separable operation Λ on a bipartite quantum system is a transformation of the form

$$\rho' = \Lambda(\rho) = \sum_m (A_m \otimes B_m)\rho(A_m^\dagger \otimes B_m^\dagger), \tag{2.1}$$

where ρ is an initial density operator on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The Kraus operators $A_m \otimes B_m$ are arbitrary product operators satisfying the closure condition

$$\sum_m A_m^\dagger A_m \otimes B_m^\dagger B_m = I \otimes I. \tag{2.2}$$

The extension of (2.1) and (2.2) to multipartite systems is obvious, but here we will only consider the bipartite case. To avoid technical issues the sums in (2.1) and (2.2) and the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ are assumed to be finite.

Various kinds of separable operations play important roles in quantum information theory. When m takes on only one value the operators A_1 and B_1 are (or can be chosen to be) unitary operators, and the operation is a *local unitary* transformation. When every A_m and every B_m is proportional to a unitary operator, we call the operation a *separable random unitary channel*. Both of these are members of the well-studied class of *local operations with classical communication* (LOCC), which can be thought of as an operation carried out by Alice on $\mathcal{H}_A$ with the outcome communicated to Bob. He then uses this information to choose an operation that is carried out on $\mathcal{H}_B$, with outcome communicated to Alice, who uses it to determine the next operation on $\mathcal{H}_A$, and so forth. For a precise definition and a discussion, see [[HHHH09], Sec. XI]. While any LOCC is a separable operation, i.e., can be written in the form (2.1), the reverse is not true: there are separable operations which fall outside the LOCC class [BDF$^+$99].

Studying properties of general separable operations seems worthwhile because any results obtained this way then apply to the LOCC subcategory, which is harder to characterize from a mathematical point of view. However, relatively little is known about separable operations, whereas LOCC has been the subject of intensive studies, with many important results. For example, an LOCC applied to a pure entangled state $|\psi\rangle$ (i.e., $\rho = |\psi\rangle\langle\psi|$ in (2.1)) results in an ensemble of pure states (labeled by m) whose average entanglement cannot exceed that of $|\psi\rangle$, [[HHHH09], Sec. XV D]. One suspects that the same is true of a general separable operation Λ, but this has not been proved. All that seems to be known is that Λ cannot "generate" entanglement when applied to a

product pure state or a separable mixed state: the outcome (as is easily checked) will be a separable state.

If an LOCC is applied to a pure (entangled) state $|\psi\rangle$, Lo and Popescu [LP01] have shown that the same result, typically an ensemble, can be achieved using a different LOCC (depending both on the original operation and on $|\psi\rangle$) in which Alice carries out an appropriate operation on $\mathcal{H}_A$ and Bob a unitary, depending on that outcome, on $\mathcal{H}_B$. This in turn is the basis of a condition due to Nielsen [Nie99] which states that there is an LOCC operation deterministically (probability 1) mapping a given bipartite state $|\psi\rangle$ to another pure state $|\phi\rangle$ if and only if $|\phi\rangle$ majorizes $|\psi\rangle$ [1].

In this chapter we derive a necessary condition for a separable operation to deterministically map $|\psi\rangle$ to $|\phi\rangle$ in terms of their Schmidt coefficients, the inequality (2.5). While it is weaker than Nielsen's condition (unless either $\mathcal{H}_A$ or $\mathcal{H}_B$ is two dimensional, in which case it is equivalent), it is not trivial. In the particular case that the Schmidt coefficients are the same, i.e., $|\psi\rangle$ and $|\phi\rangle$ are equivalent under local unitaries, we show that all the A_m and B_m operators in (2.1) are proportional to unitaries, so that in this case the separable operation is also a random unitary channel. For this situation we also study the conditions under which a whole *collection* $\{|\psi_j\rangle\}$ of pure states are deterministically mapped to pure states, a problem which seems not to have been previously studied either for LOCC or for more general separable operations.

The remainder of this chapter is organized as follows. Section 2.2 has the proof, based on a inequality by Minkowski, p. 482 of [HJ99], of the relationship between the Schmidt coefficients of $|\psi\rangle$ and $|\phi\rangle$ when a separable operation deterministically maps $|\psi\rangle$ to $|\phi\rangle$, and some consequences of this result. In Section 2.3 we derive and discuss the conditions under which a separable random unitary channel will map a collection of pure states to pure states. A summary and some discussion of open questions will be found in Section 2.4.

2.2 Local transformations of bipartite entangled states

We use the term *Schmidt coefficients* for the *nonnegative* coefficients $\{\lambda_j\}$ in the Schmidt expansion

$$|\psi\rangle = \sum_{j=0}^{D-1} \sqrt{\lambda_j}|a_j\rangle \otimes |b_j\rangle, \tag{2.3}$$

of a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, using appropriately chosen orthonormal bases $\{|a_j\rangle\}$ and $\{|b_j\rangle\}$, with the order chosen so that

$$\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{D-1} \geq 0. \tag{2.4}$$

The number r of positive (nonzero) Schmidt coefficients is called the *Schmidt rank*. We call the subspace of $\mathcal{H}_A$ spanned by $|a_0\rangle, |a_1\rangle \ldots |a_{r-1}\rangle$, i.e., the basis kets for which the Schmidt coefficients are positive, the $\mathcal{H}_A$ *support* of $|\psi\rangle$, and that spanned by $|b_0\rangle, |b_1\rangle \ldots |b_{r-1}\rangle$ its $\mathcal{H}_B$ *support*.

Our main result is the following:

Theorem 2.1. *Let $|\psi\rangle$ and $|\phi\rangle$ be two bipartite entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$ with positive Schmidt coefficients $\{\lambda_j\}$ and $\{\mu_j\}$, respectively, in decreasing order, and let r be the Schmidt rank of $|\psi\rangle$. If $|\psi\rangle$ can be transformed to $|\phi\rangle$ by a deterministic separable operation, then*

i) The Schmidt rank of $|\phi\rangle$ is less than or equal to r.

ii)

$$\prod_{j=0}^{r-1} \lambda_j \geq \prod_{j=0}^{r-1} \mu_j. \tag{2.5}$$

[1] By "$|\phi\rangle$ majorizes $|\psi\rangle$" we mean that the vector of eigenvalues of the reduced density operator $\rho(\phi)$ of $|\phi\rangle$ on $\mathcal{H}_A$ majorizes that of the reduced density operator $\rho(\psi)$ of $|\psi\rangle$ in the sense discussed in [Nie99], or in [[NC00], Sec. 12.5.1]: the sum of the k largest eigenvalues of $\rho(\phi)$ is never smaller than the corresponding sum for $\rho(\psi)$. A helpful discussion of majorization is also found in [HJ99] (see the index), with, however, the opposite convention from Nielsen for "A majorizes B"

iii) If (2.5) *is an equality with both sides positive, the Schmidt coefficients of* $|\psi\rangle$ *and* $|\phi\rangle$ *are identical,* $\lambda_j = \mu_j$*, and the operators* A_m *and* B_m *restricted to the* $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *supports of* $|\psi\rangle$*, respectively, are proportional to unitary operators.*

iv) The reverse deterministic transformation of $|\phi\rangle$ *to* $|\psi\rangle$ *by a separable operation is only possible when the Schmidt coefficients are identical,* $\lambda_j = \mu_j$*.*

Proof. For the proof it is convenient to use map-state duality (see [ZB04, GWYC06] and [[BZ06], Chap. 11]) defined in the following way. Let $\{|b_j\rangle\}$ b e an orthonormal basis of $\mathcal{H}_B$ that will remain fixed throughout the following discussion. Any ket $|\chi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be expanded in this basis in the form

$$|\chi\rangle = \sum_j |\alpha_j\rangle \otimes |b_j\rangle, \tag{2.6}$$

where the $\{|\alpha_j\rangle\}$ are the (unnormalized) expansion coefficients. We define the corresponding dual map $\chi : \mathcal{H}_B \to \mathcal{H}_A$ to be

$$\chi = \sum_j |\alpha_j\rangle \langle b_j| . \tag{2.7}$$

Obviously any map from $\mathcal{H}_B$ to $\mathcal{H}_A$ can be written in the form (2.7), and can thus be transformed into a ket on $\mathcal{H}_A \otimes \mathcal{H}_B$ by the inverse process: replacing $\langle b_j|$ with $|b_j\rangle$. The transformation depends on the choice of basis $\{|b_j\rangle\}$, but this will not matter, because our results will in the end be independent of this choice. Note in particular that the *rank* of the operator χ is exactly the same as the *Schmidt rank* of $|\chi\rangle$.

For a separable operation that deterministically maps $|\psi\rangle$ to $|\phi\rangle$ (or, to be more specific, $|\psi\rangle\langle\psi|$ to $|\phi\rangle\langle\phi|$) it must be the case that

$$\big(A_m \otimes B_m\big)|\psi\rangle = \sqrt{p_m}|\phi\rangle, \tag{2.8}$$

for every m, as otherwise the result of the separable operation acting on $|\psi\rangle$ would be a mixed state. (One could also include a complex phase factor depending on m, but this can be removed by incorporating it in A_m—an operation is not changed if the Kraus operators are multiplied by phases.) By using map-state duality we may rewrite (2.8) in the form

$$A_m \psi \bar{B}_m = \sqrt{p_m}\phi, \tag{2.9}$$

where by $\bar{B}_m$ we mean the *transpose* of this operator in the basis $\{|b_j\rangle\}$—or, to be more precise, the operator whose matrix in this basis is the transpose of the matrix of B_m. From (2.9) one sees at once that since the rank of a product of operators cannot be larger than the rank of any of the factors, the rank of ϕ cannot be greater than that of ψ. When translated back into Schmidt ranks this proves (i).

For the next part of the proof let us first assume that $\mathcal{H}_A$ and $\mathcal{H}_B$ have the same dimension D, and that the Schmidt ranks of both $|\psi\rangle$ and $|\phi\rangle$ are equal to D; we leave until later the modifications necessary when these conditions are not satisfied. In light of the previous discussion of (2.9), we see that $\bar{B}_m$ has rank D, so is invertible. Therefore one can solve (2.9) for A_m, and if the solution is inserted in (2.2) the result is

$$I \otimes I = \sum_m p_m \big[\psi^{-1\dagger} \bar{B}_m^{-1\dagger} (\phi^\dagger \phi) \bar{B}_m^{-1} \psi^{-1}\big] \otimes \big[B_m^\dagger B_m\big] \tag{2.10}$$

The Minkowski inequality ([HJ99], p. 482) for a sum of positive semidefinite operators on a S-dimensional space is

$$\left[\det\Big(\sum_m Q_m\Big)\right]^{1/S} \geq \sum_m \Big(\det Q_m\Big)^{1/S}, \tag{2.11}$$

with equality if and only if all Q_m's are proportional, i.e. $Q_i = f_{ij}Q_j$, where the f_{ij} are positive constants. Since $A_m^\dagger A_m \otimes B_m^\dagger B_m$ is a positive operator on a $S = D^2$ dimensional space, (2.10) and (2.11) yield

$$\begin{aligned} 1 &\geq \left[\det\Big(\sum_m p_m \big[\psi^{-1\dagger} \bar{B}_m^{-1\dagger} (\phi^\dagger\phi) \bar{B}_m^{-1} \psi^{-1}\big] \otimes \big[B_m^\dagger B_m\big] \Big) \right]^{1/D^2} \\ &\geq \sum_m \left[\det\Big(p_m \big[\psi^{-1\dagger} \bar{B}_m^{-1\dagger} (\phi^\dagger\phi) \bar{B}_m^{-1} \psi^{-1}\big] \otimes \big[B_m^\dagger B_m\big] \Big) \right]^{1/D^2} \\ &= \sum_m p_m \frac{\det(\phi^\dagger\phi)^{1/D}}{\det(\psi^\dagger\psi)^{1/D}} = \frac{\det(\phi^\dagger\phi)^{1/D}}{\det(\psi^\dagger\psi)^{1/D}}, \end{aligned} \tag{2.12}$$

which is equivalent to

$$\det(\psi^\dagger\psi) \geq \det(\phi^\dagger\phi). \tag{2.13}$$

The relation $\det(A \otimes B)$=$(\det A)^b(\det B)^a$, where a, b are the dimensions of A and B, was used in deriving (2.12). Since (2.13) is the square of (2.5), this proves part (ii).

If (2.5) is an equality with both sides positive, $\det(\phi^\dagger\phi)/\det(\psi^\dagger\psi) = 1$ and the inequality (2.12) becomes an equality, which implies that all positive operators in (2.11) are proportional, i.e.

$$A_m^\dagger A_m \otimes B_m^\dagger B_m = f_{mn} A_n^\dagger A_n \otimes B_n^\dagger B_n, \tag{2.14}$$

where the f_{mn} are positive constants. Setting $n = 1$ in (2.14) and inserting it in (2.2) one gets

$$(\sum_m f_{m1}) A_1^\dagger A_1 \otimes B_1^\dagger B_1 = I \otimes I. \tag{2.15}$$

This implies that both $A_1^\dagger A_1$ and $B_1^\dagger B_1$ are proportional to the identity, so A_1 and B_1 are proportional to unitary operators, and of course the same argument works for every m. Since local unitaries cannot change the Schmidt coefficients, it is obvious that $|\psi\rangle$ and $|\phi\rangle$ must share the same set of Schmidt coefficients, that is $\lambda_j = \mu_j$, for every j, and this proves (iii).

To prove (iv), note that if there is a separable operation carrying $|\psi\rangle$ to $|\phi\rangle$ and another carrying $|\phi\rangle$ to $|\psi\rangle$, the Schmidt ranks of $|\psi\rangle$ and $|\phi\rangle$ must be equal by (i), and (2.5) is an equality, so (iii) implies equal Schmidt coefficients.

Next let us consider the modifications needed when the Schmidt ranks of $|\psi\rangle$ and $|\phi\rangle$ might be unequal, and are possibly less than the dimensions of $\mathcal{H}_A$ or $\mathcal{H}_B$, which need not be the same. As noted previously, (2.9) shows that the Schmidt rank of $|\phi\rangle$ cannot be greater than that of $|\psi\rangle$. If it is less, then the right side of (2.5) is zero, because at least one of the μ_j in the product will be zero, so part (ii) of the theorem is automatically satisfied, part (iii) does not apply, and (iv) is trivial. Thus we only need to discuss the case in which the Schmidt ranks of $|\psi\rangle$ and $|\phi\rangle$ have the same value r. Let P_A and P_B be the projectors on the $\mathcal{H}_A$ and $\mathcal{H}_B$ supports $\mathcal{S}_A$ and $\mathcal{S}_B$ of $|\psi\rangle$ (as defined at the beginning of this section), and let $\mathcal{T}_A$ and $\mathcal{T}_B$ be the corresponding supports of $|\phi\rangle$. Note that each of these subspaces is of dimension r. Since $(P_A \otimes P_B)|\psi\rangle = |\psi\rangle$, (2.8) can be rewritten as

$$\big(A'_m \otimes B'_m\big)|\psi\rangle = \sqrt{p_m}|\phi\rangle, \tag{2.16}$$

where

$$A'_m = A_m P_A, \quad B'_m = B_m P_B \tag{2.17}$$

are the operators A_m and B_m restricted to the supports of $|\psi\rangle$. In fact, A'_m maps $\mathcal{S}_A$ onto $\mathcal{T}_A$, and B'_m maps $\mathcal{S}_B$ onto $\mathcal{T}_B$, as this is the only way in which (2.16) can be satisfied when $|\phi\rangle$ and $|\psi\rangle$ have

the same Schmidt rank. Finally, by multiplying (2.2) by $P_A \otimes P_B$ on both left and right one arrives at the closure condition

$$\sum_m {A'_m}^\dagger A'_m \otimes {B'_m}^\dagger B'_m = P_A \otimes P_B. \tag{2.18}$$

Thus if we use the restricted operators A'_m and B'_m we are back to the situation considered previously, with $\mathcal{S}_A$ and $\mathcal{T}_A$ (which are isomorphic) playing the role of $\mathcal{H}_A$, and $\mathcal{S}_B$ and $\mathcal{T}_B$ the role of $\mathcal{H}_B$, and hence the previous proof applies. □

Some connections between LOCC and the more general category of separable operations are indicated in the following corollaries:

Corollary 2.2. *When $|\psi\rangle$ is majorized by $|\phi\rangle$, so there is a deterministic LOCC mapping $|\psi\rangle$ to $|\phi\rangle$, there does not exist a separable operation that deterministically maps $|\phi\rangle$ to $|\psi\rangle$, unless these have equal Schmidt coefficients (are equivalent under local unitaries).*

This is nothing but (iv) of Theorem 1 applied when the $|\psi\rangle$ to $|\phi\rangle$ map is LOCC, and thus separable. It is nonetheless worth pointing out because majorization provides a very precise characterization of what deterministic LOCC operations can accomplish, and the corollary provides a connection with more general separable operations.

Corollary 2.3. *If either $\mathcal{H}_A$ or $\mathcal{H}_B$ is 2-dimensional, then $|\psi\rangle$ can be deterministically transformed to $|\phi\rangle$ if and only if this is possible using LOCC, i.e., $|\psi\rangle$ is majorized by $|\phi\rangle$.*

The proof comes from noting that when there are only two nonzero Schmidt coefficients, the majorization condition is $\mu_0 \geq \lambda_0$, and this is equivalent to (2.5).

2.3 Separable random unitary channel

2.3.1 Condition for deterministic mapping

Any quantum operation (trace-preserving completely positive map) can be thought of as a quantum channel, and if the Kraus operators are proportional to unitaries, the channel is bistochastic (maps I to I) and is called a random unitary channel or a random external field in Sec. 10.6 of [BZ06]. Thus a separable operation in which the A_m and B_m are proportional to unitaries U_m and V_m, so (2.1) takes the form

$$\rho' = \Lambda(\rho) = \sum_m p_m \big(U_m \otimes V_m\big)\rho\big(U_m \otimes V_m\big)^\dagger, \tag{2.19}$$

with the $p_m > 0$ summing to 1, can be called a separable random unitary channel. We shall be interested in the case in which $\mathcal{H}_A$ and $\mathcal{H}_B$ have the same dimension D, and in which the separable unitary channel deterministically maps not just one but a collection $\{|\psi_j\rangle\}$, $1 \leq j \leq N$ of pure states of full Schmidt rank D to pure states. This means that (2.8) written in the form

$$\big(U_m \otimes V_m\big)|\psi_j\rangle \doteq |\phi_j\rangle, \tag{2.20}$$

must hold for all j as well as for all m. The dot equality $\doteq$ means the two sides can differ by at most a complex phase. Here such phases cannot simply be incorporated in U_m or V_m, because (2.20) must hold for all values of j, even though they are not relevant for the map carrying $|\psi_j\rangle\langle\psi_j|$ to $|\phi_j\rangle\langle\phi_j|$.

Theorem 2.4. *Let $\{|\psi_j\rangle\}$, $1 \leq j \leq N$ be a collection of states of full Schmidt rank on a tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of two spaces of equal dimension, and let Λ be the separable random unitary channel defined by* (2.19)*. Let ψ_j and ϕ_j be the operators dual to $|\psi_j\rangle$ and $|\phi_j\rangle$—see* (2.6) *and* (2.7)*.*

i) If every $|\psi_j\rangle$ from the collection is deterministically mapped to a pure state, then

$$U_m^\dagger U_n \psi_j \psi_k^\dagger \doteq \psi_j \psi_k^\dagger U_m^\dagger U_n \tag{2.21}$$

for every $m, n, j,$ and k.

ii) If (2.21) *holds for a* fixed *m and every $n, j,$ and k, it holds for every $m, n, j,$ and k. If in addition* at least one *of the states from the collection $\{|\psi_j\rangle\}$ is deterministically mapped to a pure state by Λ, then every state in the collection is mapped to a pure state.*

iii) Statements (i) and (ii) also hold when (2.21) *is replaced with*

$$V_m^\dagger V_n \psi_j^\dagger \psi_k \doteq \psi_j^\dagger \psi_k V_m^\dagger V_n. \tag{2.22}$$

Proof. Part (i). By map-state duality (2.20) can be rewritten as

$$U_m \psi_j \bar{V}_m \doteq \phi_j, \tag{2.23}$$

where $\bar{V}_m$ is the transpose of V_m—see the remarks following (2.9). By combining (2.23) with its adjoint with j replaced by k, and using the fact that $\bar{V}_m$ is unitary, we arrive at

$$U_m \psi_j \psi_k^\dagger U_m^\dagger \doteq \phi_j \phi_k^\dagger. \tag{2.24}$$

Since the right side is independent of m, so is the left, which means that

$$U_n \psi_j \psi_k^\dagger U_n^\dagger \doteq U_m \psi_j \psi_k^\dagger U_m^\dagger. \tag{2.25}$$

Multiply on the left by $U_m^\dagger$ and on the right by U_n to obtain (2.21).

Part (ii). If (2.25), which is equivalent to (2.21), holds for $m = 1$ it obviously holds for all values of m. Now assume that $|\psi_1\rangle$ is mapped by Λ to a pure state $|\phi_1\rangle$, so (2.23) holds for all m when $j = 1$. Take the adjoint of this equation and multiply by $\bar{V}_m$ to obtain

$$\psi_1^\dagger U_m^\dagger \doteq \bar{V}_m \phi_1^\dagger. \tag{2.26}$$

Set $k = 1$ in (2.25), and use (2.26) to rewrite it as

$$U_n \psi_j \bar{V}_n \phi_1^\dagger \doteq U_m \psi_j \bar{V}_m \phi_1^\dagger. \tag{2.27}$$

Since by hypothesis $|\psi_1\rangle$ has Schmidt rank D, the same is true of ψ_1, and since U_m and $\bar{V}_m$ in (2.23) are unitaries, ϕ_1 and thus also $\phi_1^\dagger$ has rank D and is invertible. Consequently, (2.27) implies that

$$U_n \psi_j \bar{V}_n \doteq U_m \psi_j \bar{V}_m, \tag{2.28}$$

and we can define ϕ_j to be one of these common values, for example $U_1 \psi_j \bar{V}_1$. Map-state duality transforms this ϕ_j into $|\phi_j\rangle$ which, because of (2.28), satisfies (2.20).

Part (iii). The roles of U_m and V_m are obviously symmetrical, but our convention for map-state duality makes ψ_j a map from $\mathcal{H}_B$ to $\mathcal{H}_A$, which is the reason why its adjoint appears in (2.22). □

2.3.2 Example

Let us apply Theorem 2.4 to see what pure states of full Schmidt rank are deterministically mapped onto pure states by the following separable random unitary channel on two qubits:

$$\Lambda(\rho) = p\rho + (1-p)(X \otimes Z)\rho(X \otimes Z). \tag{2.29}$$

The Kraus operators are $I \otimes I$ and $X \otimes Z$, so $U_1 = I$ and $U_2 = X$. Thus the condition (2.21) for a collection of states $\{|\psi_j\rangle\}$ to be deterministically mapped to pure states is

$$X \psi_j \psi_k^\dagger \doteq \psi_j \psi_k^\dagger X. \tag{2.30}$$

It is easily checked that

$$|\psi_1\rangle = (|+\rangle|0\rangle + |-\rangle|1\rangle)/\sqrt{2} \tag{2.31}$$

is mapped to itself by (2.29). If the corresponding

$$\psi_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.32}$$

is inserted in (2.30) with $k = 1$, one can show that (2.30) is satisfied for any 2×2 matrix

$$\psi_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix} \tag{2.33}$$

having $c_j = \pm a_j$ and $d_j = \mp b_j$, and that in turn these satisfy (2.30) for every j and k. Thus all states of the form

$$|\psi_\pm\rangle = a|00\rangle + b|01\rangle \pm a|10\rangle \mp b|11\rangle \tag{2.34}$$

with a and b complex numbers, are mapped by this channel into pure states.

2.4 Conclusions

Our main results are in Theorem 2.1: if a pure state on a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ is deterministically mapped to a pure state by a separable operation $\{A_m \otimes B_m\}$, then the product of the Schmidt coefficients can only decrease, and if it remains the same, the two sets of Schmidt coefficients are identical to each other, and the A_m and B_m operators are proportional to unitaries. (See the detailed statement of the theorem for situations in which some of the Schmidt coefficients vanish.) This *product condition* is necessary but not sufficient: i.e., even if it is satisfied there is no guarantee that a separable operation exists which can carry out the specified map. Indeed, we think it is likely that when both $\mathcal{H}_A$ and $\mathcal{H}_B$ have dimension 3 or more there are situations in which the product condition is satisfied but a deterministic map is not possible. The reason is that (2.5) is consistent with $|\phi\rangle$ having a larger entanglement than $|\psi\rangle$, and we doubt whether a separable operation can increase entanglement. While it is known that LOCC cannot increase the average entanglement [[HHHH09], Sec. XV D], there seems to be no similar result for general separable operations. This is an important open question.

It is helpful to compare the product condition (2.5) with Nielsen's majorization condition, which says that a deterministic separable operation of the LOCC type can map $|\psi\rangle$ to $|\phi\rangle$ if and only if $|\phi\rangle$ majorizes $|\psi\rangle$, see 1. Corollary 2.3 of Theorem 2.1 shows that the two are identical if system A or system B is 2-dimensional. Under this condition a general separable operation can deterministically map $|\psi\rangle$ to $|\phi\rangle$ only if it is possible with LOCC. This observation gives rise to the conjecture that when either A or B is 2-dimensional *any* separable operation is actually of the LOCC form. This conjecture is consistent with the fact that the well-known example [BDF$^+$99] of a separable operation that is *not* LOCC uses the tensor product of two 3-dimensional spaces. But whether separable and LOCC coincide even in the simple case of a 2×2 system is at present an open question (see note added in proof).

When the dimensions of A and B are both 3 or more the product condition of Theorem 2.1 is weaker than the majorization condition: if $|\phi\rangle$ majorizes $|\psi\rangle$ then (2.5) will hold [2], but the converse is in general not true. Thus there might be situations in which a separable operation deterministically maps $|\psi\rangle$ to $|\phi\rangle$ even though $|\phi\rangle$ does not majorize $|\psi\rangle$. If such cases exist, Corollary 2.2 of Theorem 2.1 tells us that $|\psi\rangle$ and $|\phi\rangle$ must be incomparable under majorization: neither one majorizes the other. Finding an instance, or demonstrating its impossibility, would help clarify how general separable operations differ from the LOCC subclass.

[2] The general argument that (2.5) is implied by (though it does not imply) majorization will be found in [[Nie], Sec. 4], or as an exercise on [[HJ99], p. 199]

When a separable operation deterministically maps $|\psi\rangle$ to $|\phi\rangle$ and the product of the two sets of Schmidt coefficients are the same, part (iii) of Theorem 2.1 tells us that the collections of Schmidt coefficients are in fact identical, and that the A_m and B_m operators (restricted if necessary to the supports of $|\psi\rangle$) are proportional to unitaries. Given this proportionality (and that the map is deterministic), the identity of the collection of Schmidt coefficients is immediately evident, but the converse is not at all obvious. The result just mentioned can be used to simplify part of the proof in some interesting work on local copying, specifically the unitarity of local Kraus operators in [[ACP04], Sec. 3.1]. It might have applications in other cases where one is interested in deterministic nonlocal operations.

Finally, Theorem 2.4 gives conditions under which a separable random unitary operation can deterministically map a whole collection of pure states to pure states. These conditions [see (2.21) or (2.22)] involve both the unitary operators and the states themselves, expressed as operators using map-state duality, in an interesting combination. While these results apply only to a very special category, they raise the question whether simultaneous deterministic maps of several pure states might be of interest for more general separable operations. The nonlocal copying problem, as discussed in [ACP04, KE06, GKR04, OH06], is one situation where results of this type are relevant, and there may be others.

Note added in proof. Our conjecture on the equivalence of separable operations and LOCC for low dimensions has been shown to be false [DFY].

3

Separable operations on pure states

3.1 Introduction

A separable operation Λ on a bipartite quantum system is a transformation of the form

$$\rho' = \Lambda(\rho) = \sum_{k=0}^{N-1} (A_k \otimes B_k)\rho(A_k \otimes B_k)^\dagger, \tag{3.1}$$

where ρ is an initial density operator on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The Kraus operators $A_k \otimes B_k$ are arbitrary product operators satisfying the closure condition

$$\sum_{k=0}^{N-1} A_k^\dagger A_k \otimes B_k^\dagger B_k = I_A \otimes I_B, \tag{3.2}$$

with I_A and I_B the identity operators. The extension to multipartite systems is obvious, but here we will only consider the bipartite case. To avoid technical issues the sums in (3.1) and (3.2) as well as the dimensions D_A and D_B of $\mathcal{H}_A$ and $\mathcal{H}_B$ are assumed to be finite.

Local operations with classical communication (LOCC) form a subset of separable operations in which the Kraus operators $A_k \otimes B_k$ are restricted by the requirement that they be generated in the following fashion. Alice carries out an operation $\{A_i^{(1)}\}$, $\sum_i A_i^{(1)\dagger} A_i^{(1)} = I_A$, in the usual way with the help of an ancilla, the measurement of which yields the value of i, which is then transmitted to Bob. He uses i to choose an operation $\{B_j^{(2,i)}\}$, the result j of which is transmitted back to Alice, whose next operation can depend on j as well as i, and so forth. While it is (fairly) easy to see that the end result after an arbitrary number of rounds is of the form (3.1), it is difficult to characterize in simple mathematical or physical terms precisely what it is that distinguishes LOCC from more general separable operations. Examples show that separable operations can be more effective than LOCC in distinguishing certain sets of orthogonal states [BDF$^+$99], even in a system as simple as two qubits [DFY], but apart from this little is known about the difference.

What we demonstrate in Sec. 3.2 of this chapter is that the ensemble $\{p_k, |\phi_k\rangle\}$ produced by a separable operation acting on a pure state $|\psi\rangle$, see (3.5), satisfies a majorization condition (3.7), which is already known to be a necessary and sufficient condition for producing the same ensemble from the same $|\psi\rangle$ by LOCC. Among the consequences discussed in Sec. 3.3 are: a separable operation acting on a pure state can be "simulated" by LOCC; a necessary condition for a deterministic

transformation $|\psi\rangle \to |\phi\rangle$ given in [GG07] can be replaced by a necessary and sufficient majorization condition; and certain entanglement measures are nonincreasing under separable operations. Section 3.4 summarizes our main result and indicates some open questions.

3.2 Ensembles produced by separable operations on pure bipartite states

3.2.1 Majorization conditions

Let $\{A_k \otimes B_k\}_{k=1}^N$ be a separable operation on $\mathcal{H}_A \otimes \mathcal{H}_B$, specified by N Kraus operators satisfying the closure condition (3.2). Let $|\psi\rangle$ be a normalized entangled state on $\mathcal{H}_A \otimes \mathcal{H}_B$ with Schmidt form

$$|\psi\rangle = \sum_{j=0}^{D-1} \sqrt{\lambda_j}|a_j\rangle|b_j\rangle, \tag{3.3}$$

where $D = D_B$, and we assume without loss of generality that $D_A \geq D_B$. Here $\{|a_j\rangle\}$ and $\{|b_j\rangle\}$ are orthonormal bases chosen so that the Schmidt weights (coefficients) λ_j are in increasing order, i.e.

$$0 \leqslant \lambda_0 \leqslant \lambda_1 \leqslant \cdots \leqslant \lambda_{D-1}. \tag{3.4}$$

The separable operation acting on $|\psi\rangle$ will produce an ensemble $\{p_k, |\phi_k\rangle\}_{k=1}^N$, where

$$(A_k \otimes B_k)|\psi\rangle = \sqrt{p_k}|\phi_k\rangle \tag{3.5}$$

and

$$p_k = \langle\psi|A_k^\dagger A_k \otimes B_k^\dagger B_k|\psi\rangle. \tag{3.6}$$

In [JP99] it was shown that such an ensemble $\{p_k, |\phi_k\rangle\}_{k=0}^{N-1}$ can be produced from $|\psi\rangle$ by a suitable LOCC if and only if the majorization inequalities

$$\sum_{k=0}^{N-1} p_k E_n(|\phi_k\rangle) \leqslant E_n(|\psi\rangle) \tag{3.7}$$

hold for $0 \leqslant n \leqslant D-1$, where

$$E_n(|\psi\rangle) = \chi_n\big(\mathrm{Tr}_A|\psi\rangle\langle\psi|\big) = \sum_{j=0}^{n} \lambda_j, \tag{3.8}$$

and similarly for the $|\phi_k\rangle$. Here $\mathrm{Tr}_A(|\psi\rangle\langle\psi|)$ is the reduced density operator of $|\psi\rangle\langle\psi|$ on Bob's side, and $\chi_n(\cdot)$ is defined to be the sum of the first n smallest eigenvalues of its argument. Note that we are assuming that $D = D_B \leq D_A$, because if D_B were greater than D_A the extra zero eigenvalues in $\mathrm{Tr}_A|\psi\rangle\langle\psi|$ would cause confusion when using χ_n.

Our main result is the following.

Theorem 3.1. *The ensemble $\{p_k, |\phi_k\rangle\}_{k=0}^{N-1}$ can be produced by a bipartite separable operation acting on the normalized state $|\psi\rangle$ if and only if the majorization condition defined by the collection of inequalities in* (3.7) *is satisfied.*

Proof. To simplify the proof we assume that $D_A = D_B = D$. If D_A is larger, one always modify each A_k by following it with a suitable local unitary which has the result that as long as the Kraus operators are acting on a fixed $|\psi\rangle$ the action on the A side takes place in a subspace of $\mathcal{H}_A$ of

dimension D. These local unitaries do not change the Schmidt weights of the $|\phi_k\rangle$ or alter the closure condition (3.2). For more details about this "decoupling" see [GG07].

When the majorization condition (3.7) holds the result in [JP99] guarantees the existence of an LOCC (hence separable operation) which will produce the ensemble out of $|\psi\rangle$. The reverse inference, that the ensemble $\{p_k, |\phi_k\rangle\}_{k=0}^{N-1}$ defined in (3.5) and (3.6) satisfies (3.7), follows from noting that

$$p_k E_n(|\phi_k\rangle) = \chi_n\big(\mathrm{Tr}_A[A_k \otimes B_k|\psi\rangle\langle\psi| A_k^\dagger \otimes B_k^\dagger]\big), \tag{3.9}$$

and applying Theorem 3.2 below with $R = I_A \otimes I_B$, corresponding to (3.2), so $\|R\| = 1$. □

3.2.2 A majorization theorem

Theorem 3.2. *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ have the same dimension D, let $|\psi\rangle$ be some pure state on $\mathcal{H}_A \otimes \mathcal{H}_B$, and let $\{A_k \otimes B_k\}_{k=0}^{N-1}$ be any collection of product operators on $\mathcal{H}_A \otimes \mathcal{H}_B$. Then for every $0 \leqslant n \leqslant D-1$*

$$\sum_{k=0}^{N-1} \chi_n\big(\mathrm{Tr}_A[A_k \otimes B_k|\psi\rangle\langle\psi| A_k^\dagger \otimes B_k^\dagger]\big) \leqslant \|R\|\chi_n\big(\mathrm{Tr}_A|\psi\rangle\langle\psi|\big), \tag{3.10}$$

where $\|R\| = \sup_{\||\omega\rangle\|=1} \||R|\omega\rangle\|$ is the largest eigenvalue of the positive operator

$$R = \sum_{k=0}^{N-1} A_k^\dagger A_k \otimes B_k^\dagger B_k. \tag{3.11}$$

Proof. By map-state duality [GG07, ZB04, GWYC06], using the Schmidt bases of $|\psi\rangle$, we transform the state $A_k \otimes B_k|\psi\rangle$ to a map $A_k\psi\bar{B}_k$, where

$$\psi = \sum_{j=0}^{D-1} \sqrt{\lambda_j}|a_j\rangle\langle b_j|. \tag{3.12}$$

denotes an operator mapping $\mathcal{H}_B$ to $\mathcal{H}_A$, and $\bar{B}_k = B_k^T$ is the transpose of B_k. The matrix of ψ using the Schmidt bases of $|\psi\rangle$ is diagonal, with the entries on the diagonal in increasing order. (See Sec. II of [GG07] for more details on map-state duality.) Upon writing the partial traces as

$$\mathrm{Tr}_A|\psi\rangle\langle\psi| = \psi\psi^\dagger, \quad \mathrm{Tr}_A[A_k \otimes B_k|\psi\rangle\langle\psi| A_k^\dagger \otimes B_k^\dagger] = A_k\psi\bar{B}_k\bar{B}_k^\dagger\psi^\dagger A_k^\dagger, \tag{3.13}$$

the inequalities (3.10) become:

$$\sum_{k=0}^{N-1} \chi_n(A_k\psi\bar{B}_k\bar{B}_k^\dagger\psi^\dagger A_k^\dagger) \leqslant \|R\|\chi_n(\psi\psi^\dagger). \tag{3.14}$$

For some n between 0 and $D-1$ write the diagonal matrix ψ as

$$\psi = \psi_n + \tilde{\psi}_n, \tag{3.15}$$

where ψ_n is the same matrix but with $\lambda_n, \lambda_{n+1}, \ldots$ set equal to zero, while $\tilde{\psi}_n$ is obtained by setting $\lambda_0, \lambda_1, \ldots \lambda_{n-1}$ equal to zero. Lemma 3.3, below, tells us that for each k,

$$\chi_n(A_k\psi\bar{B}_k\bar{B}_k^\dagger\psi^\dagger A_k^\dagger) \leqslant \mathrm{Tr}(A_k\psi_n\bar{B}_k\bar{B}_k^\dagger\psi_n^\dagger A_k^\dagger). \tag{3.16}$$

By map-state duality,

$$\mathrm{Tr}(A_k\psi_n\bar{B}_k\bar{B}_k^\dagger\psi_n^\dagger A_k^\dagger) = \langle\psi_n|A_k^\dagger A_k \otimes B_k^\dagger B_k|\psi_n\rangle \tag{3.17}$$

where $|\psi_n\rangle$, the counterpart of ψ_n, is given by (3.3) with D replaced by n. Inserting (3.17) in (3.16) and summing over k, see (3.11), yields

$$\sum_{k=0}^{N-1} \chi_n(A_k\psi\bar{B}_k\bar{B}_k^\dagger\psi^\dagger A_k^\dagger) \leqslant \langle\psi_n|R|\psi_n\rangle \leqslant \|R\|\langle\psi_n|\psi_n\rangle = \|R\|\chi_n(\psi^\dagger\psi). \tag{3.18}$$

This establishes (3.14), which is equivalent to (3.10). □

Lemma 3.3. *Let A, B, and ψ be $D \times D$ matrices, where ψ is diagonal with nonnegative diagonal elements in increasing order, and for some $0 \leqslant n \leqslant D-1$ let ψ_n be obtained from ψ by setting all but the n smallest diagonal elements equal to 0, as in* (3.15)*. Then*

$$\chi_n(A\psi BB^\dagger\psi^\dagger A^\dagger) \leqslant \mathrm{Tr}(A\psi_n BB^\dagger\psi_n^\dagger A^\dagger). \tag{3.19}$$

Proof. The inequality

$$\chi_n(A\psi BB^\dagger\psi^\dagger A^\dagger) \leqslant \mathrm{Tr}(P_n A\psi BB^\dagger\psi^\dagger A^\dagger P_n), \tag{3.20}$$

where P_n is a projector (orthogonal projection operator) of rank at least n, follows from the fact that for any Hermitian operator T the sum of its n smallest eigenvalues is the minimum of $\mathrm{Tr}(P_nTP_n)$ over such P_n, see page 24 of [Bha97]. Choose P_n to be the projector onto the orthogonal complement of the range of $A\tilde{\psi}_n$, where $\tilde{\psi}_n = \psi - \psi_n$, as in (3.15). The rank of $A\tilde{\psi}_n$ is no larger than the rank of $\tilde{\psi}_n$, which is smaller than or equal to $D-n$. Thus the dimension of the range of $A\tilde{\psi}_n$ cannot exceed $D-n$, so the rank of P_n is at least n. By construction, $P_nA\tilde{\psi}_n = 0$, so

$$P_nA\psi = P_nA(\psi_n + \tilde{\psi}_n) = P_nA\psi_n. \tag{3.21}$$

Thus with this choice of P_n the right side of (3.20) is

$$\mathrm{Tr}(P_nA\psi_nBB^\dagger\psi_n^\dagger A^\dagger P_n), \tag{3.22}$$

and this implies (3.19), since $P_n \leqslant I$ and $A\psi_nBB^\dagger\psi_n^\dagger A^\dagger$ is positive. □

3.3 Consequences

The following are some consequences of Theorem 3.1.

i) An ensemble $\{p_k, |\phi_k\rangle\}$ can be produced by a separable operation acting on a bipartite entangled state $|\psi\rangle$ if and only if it can be produced by some LOCC acting on the same state $|\psi\rangle$.

ii) For a given bipartite $|\psi\rangle$ and separable operation $\{A_k \otimes B_k\}_{k=0}^{N-1}$ there is another operation of the form $\{\hat{A}_l \otimes U_l\}_{l=0}^{M-1}$, where the U_l are unitary operators (and the closure condition is $\sum_{l=0}^{M-1} \hat{A}_l^\dagger\hat{A}_l = I_A$), which produces the same ensemble when applied to $|\psi\rangle$. Here M could be different from N, as two Kraus operators might yield the same $|\phi_k\rangle$. For more details about the relation between the $\{A_k, B_k\}_{k=0}^{N-1}$ set and the $\{\hat{A}_l \otimes U_l\}_{k=0}^{M-1}$ set see [LP01].

iii) A deterministic transformation $|\psi\rangle \to |\phi\rangle$ by a separable operation is possible if and only if $E_n(|\phi\rangle) \leqslant E_n(|\psi\rangle)$ for every n between 0 and $D-1$, with $E_n(.)$ defined in (3.8) This is often written as $\lambda_\psi \prec \lambda_\phi$, where λ_ψ and λ_ϕ are vectors of the corresponding Schmidt weights. (This extends Theorem 1 in [GG07].)

iv) The maximum probability of success for the transformation $|\psi\rangle \to |\phi\rangle$ by a separable operation is given by

$$p_{max}^{SEP}(|\psi\rangle \to |\phi\rangle) = \min_{n\in[0,D-1]} \frac{E_n(|\psi\rangle)}{E_n(|\phi\rangle)}, \tag{3.23}$$

where $E_n(\cdot)$ was defined in (3.8).

v) An entanglement measures E defined on pure bipartite states is nonincreasing on average under separable operations, which is to say

$$E(|\psi\rangle) \geqslant \sum_{k=0}^{N-1} p_k E(|\phi_k\rangle) \tag{3.24}$$

if and only if it is similarly nonincreasing under LOCC.

vi) Let

$$\hat{E}(\rho) = \inf \sum_i p_i E(|\psi_i\rangle), \tag{3.25}$$

with the infimum over all ensembles $\{p_i, |\psi_i\rangle\}$ yielding the density operator $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$, be the convex roof extension of a pure state entanglement measure E that is monotone on pure states in the sense of (3.24). Then $\hat{E}$ is monotone on mixed states in the sense that

$$\hat{E}(\rho) \geqslant \sum_{k=0}^{N-1} p_k \hat{E}(\sigma_k) \tag{3.26}$$

for any ensemble $\{p_k, \sigma_k\}$ produced from ρ by separable operations.

The result (i) is an immediate consequence of Theorem 3.1, as the same majorization condition applies for both separable and LOCC. Then (ii), (iii), and (iv) are immediate consequences of known results, in [LP01], [Nie99], and [Vid99], respectively, for LOCC. The result (v) is an obvious consequence of (i), whereas (vi) follows from general arguments about convex roof extensions; see Sec. XV.C.2 of [HHHH09].

3.4 Conclusion

We have shown that possible ensembles of states produced by applying a separable operation to a bipartite entangled pure state can be exactly characterized through a majorization condition, the collection of inequalities (3.7) for different n. These have long been known to be necessary and sufficient conditions for producing such an ensemble using LOCC, so their extension to the full class of separable operations is not altogether surprising, even if our proof is not altogether straightforward.

Connecting the full set of separable operations with the more specialized LOCC class immediately yields several significant consequences for the former, as indicated in the list in Sec. 3.3, because much is already known about the latter. Of particular significance is that various entanglement measures are monotone, meaning they cannot increase, under separable operations—something expected on intuitive grounds, but now rigorously proved. Since such monotonicity under LOCC has long been considered a necessary, or at least a very desirable condition for any "reasonable" entanglement measure on mixed states (see Sec. XV.B of [HHHH09]), one wonders whether monotonicity under separable operations, in principle a stronger condition, might be an equally good or even superior desideratum.

Our results apply only to bipartite states, but separable operations and the LOCC subclass can both be defined for multipartite systems. Might it be that in the multipartite case the ensemble produced by applying a separable operation to a pure entangled state could also be produced by some LOCC applied to the same state? It might be, but proving it would require very different methods than used here. There are no simple multipartite analogs of the Schmidt representation (3.3), the majorization condition (3.7), or map-state duality.

Even in the bipartite case we still know very little about separable operations which are *not* LOCC, aside from the fact that they exist and can be used to distinguish certain collections of

orthogonal states more effectively than LOCC. The results in this chapter contribute only indirectly to a better understanding of this matter: looking at what a separable operation does when applied to a *single* entangled state will not help; one must ask what it does to several different states.

4

Local cloning of entangled states by separable operations

4.1 Introduction

As summarized by the "no-cloning" theorem of [WZ82], any set of quantum states can be deterministically cloned if and only if the states in the set are mutually orthogonal. When the set consists of bipartite entangled states, and the cloning is restricted to local operations and classical communication (LOCC), the problem becomes much more difficult, and further restrictions have to be imposed. The mere orthogonality of the states no longer implies that they can be (locally) cloned.

The local cloning protocol of a set of bipartite entangled states $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ is schematically represented as

$$|\psi_i\rangle^{AB} \otimes |\phi\rangle^{ab} \longrightarrow |\psi_i\rangle^{AB} \otimes |\psi_i\rangle^{ab}, \ \forall i, \tag{4.1}$$

where the letters A, a label Alice's systems and B, b label Bob's systems. Both parties are assumed to have access to ancillary qudits and may share a classical communication channel, so that in principle any LOCC operation can be performed. The state $|\phi\rangle$ is shared in advance between the parties, and it plays the role of a "blank state" on which the copy of $|\psi_i\rangle$ is to be imprinted.

The local cloning problem has recently received a great deal of attention [GKR04, ACP04, OH06, KE06, CKRR07], and was partially extended to tripartite systems in [CKK$^+$07]. The question addressed in all previous work was which sets of states $\mathcal{S}$ can be locally cloned (by LOCC) using a given blank state $|\phi\rangle$.

Note that if one can use LOCC to transform $|\phi\rangle$ into three maximally entangled states of sufficient Schmidt rank, then the local cloning of any set of bipartite orthogonal entangled states becomes trivially possible, using teleportation: Alice uses one maximally entangled state to teleport her part of $|\psi_i\rangle$ to Bob, who then distinguishes it (i.e. learns i), and next communicates the result back to Alice. Now both Alice and Bob know which state was fed into the local cloning machine. Finally they transform deterministically the two remaining maximally entangled states into $|\psi_i\rangle \otimes |\psi_i\rangle$ by LOCC, which is always possible, according to [Nie99].

Another possible scenario that uses only two entangled blank states involves using LOCC to deterministically distinguish which state $|\psi_i\rangle$ was fed into the local cloning machine, which can always be done if there are only two states in the set $\mathcal{S}$ [WSHV00]. Then, knowing the state, one can deterministically transform the two blank states into $|\psi_i\rangle \otimes |\psi_i\rangle$ (by LOCC). In this case, one needs at least two maximally entangled resource states, one for each of the two copies that must now be created, since in general the entanglement of the original state will have been destroyed in the process of distinguishing the states [Coh07].

One might hope, however, that local cloning can be performed using even less entanglement. As first shown in [GKR04], this hope is sometimes correct. Any two (and not more) two-qubit Bell states can be locally cloned using a two-qubit maximally entangled state.

This result was further extended in [ACP04] and [OH06], which considered local cloning of maximally entangled states on higher-dimensional $D \times D$ systems using a maximally entangled resource of Schmidt rank D. First, necessary and sufficient conditions for the local cloning of two maximally entangled states were provided in [ACP04], which also proved that for $D = 2$ (qubits) or $D = 3$ (qutrits), any pair of maximally entangled states can be locally cloned with a maximally entangled blank state. Whenever D is not prime the authors showed that there always exist pairs of maximally entangled states that cannot be locally cloned with a maximally entangled blank state. A generalization to more than 2 states but prime D was given in [OH06], which showed that a set of D maximally entangled states can be locally cloned using a maximally entangled resource if and only if the states in the set are locally (cyclically) shifted

$$|\psi_i\rangle = \frac{1}{\sqrt{D}} \sum_{r=0}^{D-1} |r\rangle^A |r \oplus i\rangle^B, \tag{4.2}$$

where the $\oplus$ symbol denotes addition modulo D.

Kay and Ericsson [KE06] extended the above results to the LOCC cloning of full Schmidt rank partially entangled states using a maximally entangled blank state. They presented an explicit protocol for the local cloning of a set of $D \times D$ cyclically shifted partially entangled states

$$|\psi_i\rangle = \sum_{r=0}^{D-1} \sqrt{\lambda_r} |r\rangle^A |r \oplus i\rangle^B, \tag{4.3}$$

and asserted that (4.3) is also a necessary condition for such cloning; that the states to be cloned must be of this form. Unfortunately, the proof is not correct [1], and therefore finding necessary conditions when the states are partially entangled remains an open problem.

In this chapter, we consider a set $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ of full Schmidt rank qudit (of arbitrary dimension) partially entangled states. Actually, we will begin by considering sets $\mathcal{S}$ in which only one state is required to be full Schmidt rank, and then we will see that in fact, all states in $\mathcal{S}$ must be full rank. Previous work assumed the blank state $|\phi\rangle$ to be maximally entangled, but in the present chapter we do not impose any *a priori* assumptions on $|\phi\rangle$ and find that its Schmidt rank must be at least that of the states in $\mathcal{S}$. Furthermore, we do not restrict to LOCC cloning, but allow for the more general class of separable operations — all the necessary conditions we find for separable operations will also be necessary for LOCC since the latter is a (proper) subset of the former [BDF+99].

The remainder of the chapter is organized as follows. In the next section we give a preliminary discussion and define some terms that will be used. Then, in Sec. 4.3, we turn to the characterization of clonable sets of states, where we show that $|\phi\rangle$ and all states in $\mathcal{S}$ must be full Schmidt rank,

[1] The matter was discussed with Kay [Kay06]. The fact that the argument is not correct can be observed after a careful reading of the paragraph following Eq. (3) in [KE06]. The authors claim that the local cloning of partially entangled states is equivalent to the cloning of maximally entangled states, but this statement is incorrect, because the authors implicitly modified the Kraus operators that defined the local cloning, i.e. changed A_k to $A'_k = A_k M_0$, where M_0 (defined in Eq. (3) of [KE06]) is the operator that transforms the maximally entangled state $(1/\sqrt{D}) \sum_{r=0}^{D-1} |r\rangle^A |r\rangle^B$ to the partially entangled state $|\psi_0\rangle = \sum_{r=0}^{D-1} \sqrt{\lambda_r} |r\rangle^A |r\rangle^B$. The new Kraus operators do not satisfy the closure condition anymore (necessary for a deterministic transformation), since $\sum_k {A'_k}^\dagger A'_k \otimes {B_k}^\dagger B_k = \sum_k M_0^\dagger (A_k{}^\dagger A_k) M_0 \otimes {B_k}^\dagger B_k = M_0^\dagger M_0 \otimes I \neq I \otimes I$, because M_0 is not a unitary operator (unless $|\psi_0\rangle$ is maximally entangled, case excluded).

Another way of seeing that the argument is not correct is to observe that, if the B_k operator performs the cloning of a maximally entangled state using a maximally entangled blank, as it is claimed, then B_k must be proportional to a unitary operator, see Theorem 1(iii) of [GG07] and Sec. 3.1 of [ACP04]. It then follows that the closure condition for the Kraus operators is not satisfied, with A_k as defined in Eq. (3) of [KE06].

provide additional necessary conditions on $\mathcal{S}$, and then prove the group structure of these sets. From this group structure, it is then shown that the number of states in $\mathcal{S}$ must divide D exactly, and this is followed by a proof of a necessary ("group-shifted") condition on the local cloning of a set of $D \times D$ maximally entangled states. Then, in Sec. 4.4, we further consider group-shifted sets, now allowed to be not maximally entangled, showing that a maximally entangled blank state is sufficient by giving an LOCC protocol that clones these states. This demonstrates that the necessary condition found in the previous section for cloning maximally entangled states is also sufficient for LOCC cloning. In Sec. 4.5, we provide necessary conditions on the minimum entanglement in the blank. In addition, we obtain necessary and sufficient conditions for local cloning of any set when $D = 2$ (entangled qubits), and for any group-shifted set for $D = 3$ (entangled qutrits); in both these cases we find that the blank state must be maximally entangled, even when the states to be cloned are not. For higher dimensions with these group-shifted sets, we also show that the blank must have strictly more entanglement than the states to be cloned. Finally, Sec. 4.6 provides concluding remarks as well as some open questions. Longer proofs are presented in the Appendices.

4.2 Preliminary remarks and definitions

A separable operation Λ on a bipartite quantum system $\mathcal{H}_A \otimes \mathcal{H}_B$ is a transformation that can be written as

$$\rho' = \Lambda(\rho) = \sum_{m=0}^{M-1} (A_m \otimes B_m)\rho(A_m \otimes B_m)^\dagger \tag{4.4}$$

where ρ is an initial density operator on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The Kraus operators are arbitrary product operators satisfying the closure condition

$$\sum_{m=0}^{M-1} A_m^\dagger A_m \otimes B_m^\dagger B_m = I_A \otimes I_B, \tag{4.5}$$

with I_A and I_B the identity operators. The extension to multipartite systems is obvious, but here we will only consider the bipartite case. To avoid technical issues the sums in (4.4) and (4.5), as well as the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$, are assumed to be finite.

The local cloning protocol is described as follows. Suppose Alice and Bob are two spatially separated parties, each holding a pair of quantum systems of dimension D, with Alice's systems described by a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_a$ and Bob's by $\mathcal{H}_B \otimes \mathcal{H}_b$. Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ be a set of orthogonal bipartite entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$. Let $|\phi\rangle^{ab} \in \mathcal{H}_a \otimes \mathcal{H}_b$ be another bipartite entangled state that plays the role of a resource, which we call the blank state, and is shared in advance between Alice and Bob. Their goal is to implement deterministically (i.e. with probability one) the transformation

$$|\psi_i\rangle^{AB} \otimes |\phi\rangle^{ab} \longrightarrow |\psi_i\rangle^{AB} \otimes |\psi_i\rangle^{ab}, \forall i = 0 \ldots N-1 \tag{4.6}$$

by a bipartite separable operation. Alice and Bob know exactly the states that belong to the set $\mathcal{S}$ and also know the blank state $|\phi\rangle^{ab}$, but they do not know which state will be fed to the local cloning machine described by (4.6) — the machine has to work equally well for all states in $\mathcal{S}$! Note that local cloning is defined up to local unitaries, i.e., a set $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ can be locally cloned if and only if the set $\mathcal{S}' = \{U^A \otimes V^B|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ can be locally cloned, where U^A and V^B are local unitaries. This is true because local unitaries can always be implemented deterministically at the beginning or at the end of the cloning operation.

The Schmidt coefficients of $|\psi_i\rangle^{AB}$ are labelled by $\lambda_r^{(i)}$ and by convention are sorted in decreasing order, with $\lambda_0^{(i)} \geqslant \lambda_1^{(i)} \geqslant \cdots \geqslant \lambda_{D-1}^{(i)}$ and $\sum_{r=0}^{D-1} \lambda_r^{(i)} = 1$, for all $i = 0 \ldots N-1$, and the Schmidt

coefficients of $|\phi\rangle^{ab}$ are labelled by γ_r, with $\gamma_0 \geqslant \gamma_1 \cdots \geqslant \gamma_{D-1}$ and $\sum_{r=0}^{D-1} \gamma_r = 1$. To remind the reader that the components of a vector $\vec{\lambda}$ are ordered in decreasing order we use the notation $\vec{\lambda}^{\downarrow}$.

The Schmidt rank of a bipartite state is the number of its non-zero Schmidt coefficients. We say that a state of a $D \times D$ dimensional system has full Schmidt rank if its Schmidt rank is equal to D.

We use the concept of majorization, which is a partial ordering on D-dimensional real vectors. More precisely, if $\vec{x} = (x_0, \ldots, x_{D-1})$ and $\vec{y} = (y_0, \ldots, y_{D-1})$ are two real D-dimensional vectors, we say that $\vec{x}$ is majorized by $\vec{y}$ and write $\vec{x} \prec \vec{y}$ if and only if $\sum_{j=0}^{k} x_j^{\downarrow} \leqslant \sum_{j=0}^{k} y_j^{\downarrow}$ holds for all $k = 0, \ldots, D-1$, with equality when $k = D-1$.

For two $D \times D$ bipartite pure states $|\chi\rangle$ and $|\eta\rangle$, we use the shorthand notation $|\chi\rangle \prec |\eta\rangle$ to denote the fact that the vector of Schmidt coefficients of $|\chi\rangle$ is majorized by the vector of Schmidt coefficients of $|\eta\rangle$. See [Nie99] or Chap. 12.5 of [NC00] for more details about majorization.

The entanglement of a $D \times D$ bipartite pure state $|\chi\rangle$ can be quantified by various entanglement measures [2], the ones used extensively in this chapter being the *entropy of entanglement*

$$E(|\chi\rangle) = -\sum_{r=0}^{D-1} \lambda_r \log_D \lambda_r \tag{4.7}$$

and the *G-concurrence* [Gou05]

$$C_G(|\chi\rangle) = D \left(\prod_{r=0}^{D-1} \lambda_r \right)^{1/D}, \tag{4.8}$$

where λ_r denotes the r-th Schmidt coefficient of $|\chi\rangle$. The base D in the logarithm in (4.7) as well as the prefactor D in (4.8) appear for normalization purposes, so that the entropy of entanglement as well as the G-concurrence of a maximally entangled state are both 1, regardless of the dimension.

4.3 Characterizing sets of clonable states

4.3.1 Preliminary analysis

Mathematically, the local cloning problem can be formulated in terms of a separable transformation on a set of pure input states $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$, using a blank state $|\phi\rangle^{ab}$.

If a set of states $\mathcal{S}$ can be locally cloned using the blank state $|\phi\rangle^{ab}$, then there must exist a bipartite separable operation Λ for which

$$\Lambda(|\psi_i\rangle\langle\psi_i|^{AB} \otimes |\phi\rangle\langle\phi|^{ab}) = |\psi_i\rangle\langle\psi_i|^{AB} \otimes |\psi_i\rangle\langle\psi_i|^{AB}, \ \forall i = 0 \ldots N-1 \tag{4.9}$$

(note here that an overall phase factor in the definition of the individual states is of no significance). Since Λ is separable, it can be represented by a set of product Kraus operators,

$$\begin{aligned} &\sum_{m=0}^{M-1} (A_m \otimes B_m)(|\psi_i\rangle\langle\psi_i|^{AB} \otimes |\phi\rangle\langle\phi|^{ab})(A_m \otimes B_m)^\dagger \\ &\qquad = |\psi_i\rangle\langle\psi_i|^{AB} \otimes |\psi_i\rangle\langle\psi_i|^{AB}, \ \forall i = 0 \ldots N-1, \end{aligned} \tag{4.10}$$

where operators A_m act on $\mathcal{H}_A \otimes \mathcal{H}_a$, and B_m on $\mathcal{H}_B \otimes \mathcal{H}_b$. The above equation is equivalent to

$$\begin{aligned} &A_m \otimes B_m(|\psi_i\rangle^{AB} \otimes |\phi\rangle^{ab}) = \sqrt{p_{mi}} \mathrm{e}^{\mathrm{i}\varphi_{mi}} (|\psi_i\rangle^{AB} \otimes |\psi_i\rangle^{ab}), \\ &\quad \forall i = 0 \ldots N-1, \ \forall m = 0 \ldots M-1 \end{aligned} \tag{4.11}$$

[2] Often called entanglement monotones, i.e., non-increasing under local operations and classical communication (LOCC).

where $e^{i\varphi_{mi}}$ is a complex phase that may depend on m and i, and p_{mi} are probabilities for which

$$\sum_{m=0}^{M-1} p_{mi} = 1, \ \forall i = 0 \dots N-1. \tag{4.12}$$

By map-state duality in the computational basis [3] [ZB04, GWYC06, GG07, GG08] one can rewrite (4.11) as

$$A_m(\psi_i \otimes \phi)B_m^T = \sqrt{p_{mi}}e^{i\varphi_{mi}}\psi_i \otimes \psi_i, \ \forall i, m, \tag{4.13}$$

where ψ_i and ϕ are now operators obtained from the corresponding kets by turning a ket into a bra, and B_m^T is the transpose of B_m.

The superscripts in (4.13) that label the Hilbert spaces have been dropped for clarity, since now one can regard everything as abstract linear operators, or matrices in the computational basis. Although map-state duality is basis-dependent, our results will not depend on the choice of a specific basis.

We now state our first result characterizing sets of states $\mathcal{S}$ that can be locally cloned.

Theorem 4.1 (Rank of states in $\mathcal{S}$)**.** *Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}_{i=0}^{N-1}$ be a set of bipartite orthogonal states on $\mathcal{H}_A \otimes \mathcal{H}_B$ with one state, say $|\psi_0\rangle$, having full Schmidt rank. If the local cloning of $\mathcal{S}$ is possible by a separable operation using a blank state $|\phi\rangle$, then $|\phi\rangle$ and all states in $\mathcal{S}$ must be full rank.*

Proof. This result follows directly from (4.13). If $|\psi_0\rangle$ has full Schmidt rank, then ψ_0 is a full rank operator. Then, since the rank of a tensor product is the product of ranks, it must be that ϕ is also full rank, as are A_m and B_m for each m (a product of operators cannot have rank exceeding that of any of the individual operators in the product). Since the rank of a product of two operators is equal to that of the first whenever the second is full rank, (4.13) with $i \neq 0$ directly implies that ψ_i has full rank for every i, and we are done. □

In this chapter, we are considering sets $\mathcal{S}$ in which at least one state is full rank. Therefore by this theorem, we may instead restrict to sets in which every state is full rank, and we will do so throughout the remainder of the chapter.

As just argued in the proof of the previous theorem, all operators in (4.13) are full rank, hence invertible. Now take the inverse of (4.13), replace i by j, and right multiply (4.13) by it to obtain

$$A_m(\psi_i\psi_j^{-1} \otimes I)A_m^{-1} = \sqrt{\frac{p_{mi}}{p_{mj}}}e^{i(\varphi_{mi}-\varphi_{mj})}(\psi_i\psi_j^{-1} \otimes \psi_i\psi_j^{-1}). \tag{4.14}$$

Define

$$T_{ij}^{(m)} = \sqrt{\frac{p_{mi}}{p_{mj}}}e^{i(\varphi_{mi}-\varphi_{mj})}\psi_i\psi_j^{-1} \tag{4.15}$$

so that (4.14) can be written more compactly as

$$A_m(T_{ij}^{(m)} \otimes I)A_m^{-1} = T_{ij}^{(m)} \otimes T_{ij}^{(m)}. \tag{4.16}$$

Since for every i, ψ_i is full rank, we see that $\det(\psi_i) \neq 0$, so $\det(T_{ij}^{(m)})$ is also non-vanishing. Thus, taking the determinant on both sides of (4.16) yields

$$\det(T_{ij}^{(m)})^D = 1, \tag{4.17}$$

[3] As an example of map-state duality, a bipartite state $|\chi\rangle^{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, $|\chi\rangle^{AB} = \sum c_{ij}|i\rangle^A|j\rangle^B$, is transformed into a map $\chi : \mathcal{H}_B \longrightarrow \mathcal{H}_A$, $\chi = \sum c_{ij}|i\rangle^A\langle j|^B$. Note that the rank of the operator χ is the Schmidt rank of $|\chi\rangle^{AB}$, and the squares of the singular values of χ (or, equivalently, the eigenvalues of $\chi\chi^\dagger$) are the Schmidt coefficients of $|\chi\rangle^{AB}$. For more details about map-state duality see Sec. II of [GG07].

where we have used the fact that $\det(A\otimes B)=\det(A)^M\det(B)^N$, for A and B being $N\times N$ and $M\times M$ matrices, respectively. Recalling the definition of $T_{ij}^{(m)}$ in (4.15), this condition becomes

$$1=\left(\frac{p_{mi}}{p_{mj}}\right)^{D/2}\left|\frac{\det(\psi_i)}{\det(\psi_j)}\right|, \tag{4.18}$$

or

$$p_{mj}=p_{mi}\left|\frac{\det(\psi_i)}{\det(\psi_j)}\right|^{2/D}. \tag{4.19}$$

Summing (4.19) over m yields

$$|\det(\psi_i)|=|\det(\psi_j)|\,, \tag{4.20}$$

implying

$$p_{mi}=p_{mj}, \tag{4.21}$$

hence these determinants and probabilities are independent of the input state. As a consequence, we may write $T_{ij}^{(m)}$ in the simpler form,

$$T_{ij}^{(m)}=\mathrm{e}^{\mathrm{i}(\varphi_{mi}-\varphi_{mj})}\psi_i\psi_j^{-1}. \tag{4.22}$$

Observation: The fact that $p_{mi}=p_m$, independent of i, implies that the cloning apparatus provides no information whatsoever about which state was input to that apparatus, nor can any such information "leak" to an external environment that might be used to implement the local cloning separable operation. This is not without interest, since it rules out the possibility of local cloning by locally distinguishing while preserving entanglement [Coh07]. This result turns out to be valid in the much more general setting of one-to-one transformation of full Schmidt rank pure state ensembles by separable operations, but a discussion of these broader implications will be presented in a future publication.

We can now provide additional conditions that must hold in order for $\mathcal{S}$ to be a set of states that can be locally cloned by separable operations. These are stated in the following theorem, which holds under completely general conditions, applicable for any N and D.

Theorem 4.2 (Necessary conditions)**.** *Let $\mathcal{S}=\{|\psi_i\rangle^{AB}\}$ be a set of full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A\otimes\mathcal{H}_B$. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab}\in\mathcal{H}_a\otimes\mathcal{H}_b$ is possible by a separable operation, then the following must hold:*

i) All states in $\mathcal{S}$ are equally entangled with respect to the G-concurrence measure,

$$C_G(|\psi_i\rangle^{AB})=C_G(|\psi_j\rangle^{AB}),\ \forall i,j. \tag{4.23}$$

ii) Any two states in $\mathcal{S}$ must either share the same set of Schmidt coefficients or be incomparable under majorization.

iii)

$$\mathrm{Spec}(T_{ij}^{(m)}\otimes I)=\mathrm{Spec}(T_{ij}^{(m)}\otimes T_{ij}^{(m)}),\ \forall i,j, \tag{4.24}$$

where Spec$(\cdot)$ denotes the spectrum of its argument and $T_{ij}^{(m)}$ is defined as in (4.22)*.*

Proof. Proof of i) This follows at once from (4.20), the definition (4.8) of G-concurrence, and the fact that for any state $|\chi\rangle$ the product of its Schmidt coefficients is equal to $|\det(\chi)|^2$.

Proof of ii) The proof follows from Theorem 1 (ii,iii) of [GG07] which states that any two bipartite states $|\chi\rangle$ and $|\eta\rangle$ that are comparable under majorization (i.e. $|\chi\rangle\prec|\eta\rangle$ or $|\eta\rangle\prec|\chi\rangle$) and have equal G-concurrence must share the same set of Schmidt coefficients.

Proof of iii) The proof follows at once from (4.16). □

4.3.2 Characterization of clonable sets in terms of finite groups

We next show that to any set $\mathcal{S}$ of states that can all be cloned by the same apparatus, there can be associated a finite group, and the set is essentially generated by this group.

Theorem 4.3 (Group structure of $\mathcal{S}$)**.** *Let $\mathcal{S} = \{|\psi_i\rangle^{AB}\}$ be a set of full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$. If the local cloning of $\mathcal{S}$ is possible by a separable operation, then the set $\mathcal{S}$ can be extended to a larger set such that $\{T_{ij}^{(m)}\}$ of (4.22) for fixed j, m constitutes an ordinary representation of a finite group, G. Since the states in $\mathcal{S}$ are related as $\mathrm{e}^{\mathrm{i}\varphi_{mi}}|\psi_i\rangle = \mathrm{e}^{\mathrm{i}\varphi_{mj}}(T_{ij}^{(m)} \otimes I_B)|\psi_j\rangle$, then the larger set, with $N = |G|$ members, is generated by the action of the group G on any individual state in the set.*

Proof. The starting point of the proof is to multiply (4.16) on the left of (4.13) (with index k) to obtain

$$A_m(T_{ij}^{(m)}\psi_k \otimes \phi)B_m^T = \sqrt{p_m}\mathrm{e}^{\mathrm{i}\varphi_{mk}}T_{ij}^{(m)}\psi_k \otimes T_{ij}^{(m)}\psi_k. \tag{4.25}$$

Using (4.22) this becomes

$$A_m(\psi_i\psi_j^{-1}\psi_k \otimes \phi)B_m^T = \sqrt{p_m}\mathrm{e}^{\mathrm{i}(\varphi_{mi}-\varphi_{mj}+\varphi_{mk})}\psi_i\psi_j^{-1}\psi_k \otimes \psi_i\psi_j^{-1}\psi_k, \tag{4.26}$$

which by map-state duality implies that the state $|\psi_i\psi_j^{-1}\psi_k\rangle$ is cloned by the same apparatus as all the states in the original set $\mathcal{S}$. Therefore $|\psi_i\psi_j^{-1}\psi_k\rangle$ — which, by considering the version of (4.26) that corresponds to states (as in (4.11)), taking the squared norm of both sides and summing over m, is seen to be normalized — must either (i) be orthogonal to the entire set $\mathcal{S}$, or (ii) it is equal to one of those original states up to an overall phase factor. If this state is orthogonal to $\mathcal{S}$, then $\mathcal{S}$ can be extended by including this state as one of its members. So assume $\mathcal{S}$ has been extended to its maximal size (since we are working in finite dimensions, this size will be finite), and then we can conclude that for every i, j, k,

$$\psi_i\psi_j^{-1}\psi_k = \mathrm{e}^{\mathrm{i}(\varphi_{ml}-\varphi_{mi}+\varphi_{mj}-\varphi_{mk})}\psi_l, \tag{4.27}$$

for some l, where the phase in the above expression has been determined by comparing (4.26) to (4.13). Next multiply this latter expression on the right by $\mathrm{e}^{-\mathrm{i}\varphi_{mn}}\psi_n^{-1}$ to obtain

$$T_{ij}^{(m)}T_{kn}^{(m)} = T_{ln}^{(m)}. \tag{4.28}$$

Hence the collection of $T_{ij}^{(m)}$ is closed under matrix multiplication, which is associative. In addition, $T_{ii}^{(m)} = I$ for every i and $T_{ij}^{(m)}T_{ji}^{(m)} = I$ for every i, j, so we see that the identity element and inverses are present, which concludes the proof that the set $\{T_{ij}^{(m)}\}$ with fixed m form a representation of a group, G. Now, the number of index pairs (i, j) is N^2, where N is the number of states in $\mathcal{S}$. However, we will now show that in fact the order $|G|$ of this group is equal to N and not N^2.

Setting $n = j$ in (4.28), we have

$$T_{ij}^{(m)}T_{kj}^{(m)} = T_{lj}^{(m)}, \tag{4.29}$$

so the product is closed even when the second index is constrained to be the same. If we set $l = j$, we see that with $T_{jj}^{(m)} = I$, then for each i there exists k such that $T_{kj}^{(m)} = (T_{ij}^{(m)})^{-1}$. Hence, for every fixed j the set $\mathcal{T}_j = \{T_{ij}^{(m)}\}$ also is a representation of G. Similarly, one can show the same holds if instead it is the first index that is held fixed. Note now that by multiplying (4.28) on the right by $(T_{kn}^{(m)})^{-1}$, and given that (4.28) holds for any i, j, k, n, we see that for every i, j, T_{ij} is a member of the group formed by the T_{kn} for fixed n. That is, the group of the T_{kn} for fixed n contains all elements T_{ij}.

Could two or more of the $T_{ij}^{(m)}$ be equal, for fixed j? We will now show this is not the case by demonstrating the linearly independence of the set $\mathcal{T}_j$. Indeed,

$$0 = \sum_{k=0}^{N-1} c_k T_{kj}^{(m)} = \sum_{k=0}^{N-1} c_k \mathrm{e}^{\mathrm{i}(\varphi_{mk}-\varphi_{mj})} \psi_k \psi_j^{-1}$$
$$\iff 0 = \sum_{k=0}^{N-1} c_k \mathrm{e}^{\mathrm{i}\varphi_{mk}} \psi_k. \tag{4.30}$$

However, the ψ_k are mutually orthogonal, $\mathrm{Tr}(\psi_k^\dagger \psi_j) = \delta_{jk}$, so this can only be satisfied if all the c_k vanish, implying that $\mathcal{T}_j$ is linearly independent, and hence, that $|G| = N$: the (maximal) number of states in $\mathcal{S}$ is equal to the order of G. □

For the remainder of the chapter, we will use labels f, g, h instead of i, j, k, where the former represent elements of the group G; the group multiplication is denoted as fg, with e the identity element. For example, instead of ψ_0 we will now write ψ_e, and in place of $T_{j0}^{(m)}$ we will simply write $T_f^{(m)}$.

We may now utilize the powerful tools of group theory to study sets $\mathcal{S}$ of clonable states, obtaining a very strong constraint on how many states any given apparatus can possibly clone. Any group G is characterized by its irreducible representations, which we denote as $\Gamma^{(\alpha)}(f),\ f \in G$, and any representation of G may be decomposed into a direct sum of irreducible representations with a given irreducible representation $\Gamma^{(\alpha)}(f)$ appearing some number n_α times in that sum. In general, a given representation may have $n_\alpha = 0$ for some α, but since here our representation is linearly independent, we know that every irreducible representation must appear at least once [YGC10].

We can use character theory [Ham89] to calculate n_α. Defining characters as $\chi(T_f^{(m)}) = \mathrm{Tr}(T_f^{(m)})$ and $\chi^{(\alpha)}(f) = \mathrm{Tr}(\Gamma^{(\alpha)}(f))$, we have that

$$n_\alpha = \frac{1}{|G|} \sum_{f \in G} \chi^{(\alpha)}(f)^* \chi(T_f^{(m)}). \tag{4.31}$$

However, by taking the trace of (4.16) and recalling that the trace of a tensor product is equal to the product of the traces, we see that $\chi(T_f^{(m)})$ is equal to either 0 or D. Since the identity element of the group, e, is always in a conjugacy class by itself ($e = gfg^{-1}$ if and only if $f = e$), then we may conclude that $\chi(T_f^{(m)})$ vanishes except when $f = e$, in which case $\chi(T_e^{(m)}) = D$. Thus, (4.31) reduces to

$$n_\alpha = \frac{D d_\alpha}{|G|}, \tag{4.32}$$

where $d_\alpha = \chi^{(\alpha)}(e)$ is the dimension of the α^{th} irreducible representation. Since in every finite group there is always the trivial irreducible representation of all ones, $\Gamma^{(t)}(f) = 1\ \forall f \in G$, where this irreducible representation has dimension $d_t = 1$, we have immediately that $n_t = D/|G|$ is an integer, implying that $N = |G|$ divides D. Thus,

Theorem 4.4 (Number of clonable states)**.** *If an apparatus can locally clone more than one state on a $D \times D$ system, where at least one (and therefore all, see Theorem 4.1) of these states has full Schmidt rank, then that apparatus can in fact clone a number of states that divides D exactly. In particular if D is prime, then any such apparatus can clone exactly D states, no more and no less.*

Now we see from (4.32) that n_α is an integer multiple of d_α. If $|G| = D$ so that $n_\alpha = d_\alpha$, we have what is known as the regular representation of G. Otherwise, our representation is a direct sum of an integer number $n_t = D/|G|$ of copies of the regular representation. As is well known,

there is always a choice of basis in which the matrices in a *unitary* regular representation appear as permutation matrices $L(f)$, with each row (column) having only a single non-zero entry equal to one. In this basis, denoted as $\{|g\rangle\}_{g\in G}$, we have that $L(f)|g\rangle = |fg\rangle$. The representation $L(f)$ is called the *left regular representation*. One can as well use the *right regular representation* $R(f)$ with $R(f)|g\rangle = |gf^{-1}\rangle$, but without loss of generality in the rest of the chapter we restrict only to $L(f)$, since for finite groups the right and left regular representations are equivalent [Mic95].

In our case the representation will generally not be unitary, so when $|G| = D$ we will have that

$$T_f^{(m)} = SL(f)S^{-1}, \tag{4.33}$$

for some invertible matrix S.

In the remainder of the chapter we restrict consideration to $|G| = D$ (or, equivalently, to $n_t = 1$), and note that all results obtained in the remainder of the chapter are valid (with small modifications) also when $|G| < D$. However, the notation becomes a bit cumbersome, so we defer detailed discussion about the $|G| < D$ case to Appendix 4.B.

4.3.3 Form of the clonable states when all are maximally entangled

It was shown in [ACP04] that when at least one of the states in $\mathcal{S}$ is maximally entangled, then all states in $\mathcal{S}$ must also be maximally entangled. In this section, we consider such sets, in which case the $T_f^{(m)}$ must all be unitary. This follows directly from the fact that when ψ_e is proportional to the identity then ψ_f is proportional to $T_f^{(m)}$, and also that $|\psi_f\rangle$ is maximally entangled if and only if ψ_f is proportional to a unitary.

We have seen that when $N = D$, then $T_f^{(m)} = SL(f)S^{-1}$ for some invertible S, and $L(f)$ is the permutation form of the regular representation of group G. However, we have

Lemma 4.5 (Unitary equivalence)**.** *For any two unitary representations T_f and $L(f)$ of a finite group G, which are equivalent in the sense that $T_f = SL(f)S^{-1}$ for some invertible matrix S, then these two representations are also equivalent by a unitary similarity transformation, $T_f = WL(f)W^\dagger$, with W unitary.*

A proof of this lemma is given in Chap. 3.3 of [Ma07], and we provide an alternative proof in Appendix 4.A.1.

What this lemma tells us is that ψ_f is proportional to $WL(f)\psi_e W^\dagger$ (since by local unitaries, ψ_e can be made proportional to the identity, we will assume here that this is the case, and then ψ_e commutes with $W^\dagger$), or

$$\begin{aligned} |\psi_f\rangle &= c_f(WL(f)\otimes W^*)\sum_{g\in G}|g\rangle^A|g\rangle^B \\ &= \frac{1}{\sqrt{D}}(W\otimes W^*)\sum_{g\in G}|fg\rangle^A|g\rangle^B, \end{aligned} \tag{4.34}$$

where W^* is the complex conjugate of W, the states $\{|g\rangle\}_{g\in G}$ are some orthonormal basis, $\langle g|h\rangle = \delta_{g,h}$, and we have omitted an unimportant overall phase (from c_f, of magnitude $D^{-1/2}$) in the last line. Note that up to unimportant local unitaries and relabeling of group elements, the set of states (4.34) can be written either as

$$|\psi_f\rangle = \frac{1}{\sqrt{D}}\sum_{g\in G}|fg\rangle^A|g\rangle^B \tag{4.35}$$

or

$$|\psi_f\rangle = \frac{1}{\sqrt{D}}\sum_{g\in G}|g\rangle^A|fg\rangle^B. \tag{4.36}$$

The states above are of a form that we will refer to as "group-shifted".

In Section 4.4, we provide an explicit LOCC protocol that accomplishes cloning of such shifted sets of states. Thus, we have

Theorem 4.6 (Maximally entangled states)**.** *A set of maximally entangled states on a $D\times D$ system can be cloned by LOCC if and only if there exists a choice of Schmidt bases shared by those states such that they have a group-shifted form, as in* (4.35) *or* (4.36)*.*

This extends the result of [OH06], which applied only for prime D.

Additionally, we remark that in our protocol presented in Sec. 4.4, there is no need for classical communication (the measurement M_r and the additional corrections Q_r appearing in that protocol can be omitted when the states to be cloned are maximally entangled). This result was first proven in [ACP04], where it was shown that the Kraus operators implementing the cloning of maximally entangled states have to be proportional to unitary operators. A completely different proof of this fact was later provided in [GG07], in which it was shown that a separable operation that maps a pure state to another pure state, both sharing the same set of Schmidt coefficients, must have its Kraus operators proportional to unitaries; in our case $|\psi_f\rangle\otimes|\phi\rangle$ and $|\psi_f\rangle\otimes|\psi_f\rangle$ do share the same set of Schmidt coefficients, since they are maximally entangled. We here have another simple proof of this result, since we have proved in Theorem 4.6 that a set of maximally entangled states must be group-shifted in order that they can be cloned, and since our protocol in Sec. 4.4 clones any set that is group-shifted without using communication.

4.3.4 Form of the clonable states when $D = 2$ (qubits)

Here, we restrict our attention to local cloning of qubit entangled states, $D = 2$. As D is prime, we know from Theorem 4.3 that exactly two states can be cloned, $\mathcal{S} = \{|\psi_e\rangle^{AB}, |\psi_g\rangle^{AB}\}$. Both are assumed to be entangled (non-product), but not maximally entangled.

Since there is only one independent Schmidt coefficient for a two-qubit state, any two such states are comparable under majorization, and then from part ii) of Theorem 4.2 it follows at once that these states have to share the same set of Schmidt coefficients. This is already a surprising result, implicitly assumed (but not proved) in recent work on local cloning of qubit states [CKRR07]. We can actually prove a stronger condition: not only do the states have to share the same set of Schmidt coefficients, but they must also share the same Schmidt basis and be of a shifted form, as summarized by the following theorem.

Theorem 4.7 (Entangled qubits)**.** *Let $\mathcal{S} = \{|\psi_e\rangle^{AB}, |\psi_g\rangle^{AB}\}$ be a set of 2 orthogonal two-qubit entangled states and let λ be the largest Schmidt coefficient of $|\psi_e\rangle^{AB}$, assumed to satisfy $1/2 < \lambda < 1$. If the local cloning of $\mathcal{S}$ using a two-qubit entangled blank state $|\phi\rangle^{ab}$ is possible by a separable operation, then, up to local unitaries (that is, the same local unitaries acting on both states), the states must either be of the form*

$$\begin{aligned} |\psi_e\rangle^{AB} &= \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B \\ |\psi_g\rangle^{AB} &= \sqrt{\lambda}|0\rangle^A|1\rangle^B + \sqrt{1-\lambda}|1\rangle^A|0\rangle^B \end{aligned} \tag{4.37}$$

or

$$\begin{aligned} |\psi_e\rangle^{AB} &= \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B \\ |\psi_g\rangle^{AB} &= \sqrt{\lambda}|1\rangle^A|0\rangle^B + \sqrt{1-\lambda}|0\rangle^A|1\rangle^B. \end{aligned} \tag{4.38}$$

Note that a relative phase $\mathrm{e}^{\mathrm{i}\vartheta}$ may be introduced into $|\psi_g\rangle$, without altering $|\psi_e\rangle$, by Alice and Bob doing local unitaries on systems A and B, $U^{A,B} = |0\rangle\langle 0| + \mathrm{e}^{\pm\mathrm{i}\vartheta/2}|1\rangle\langle 1|$ (one of them chooses the upper sign, the other does the lower, which accomplishes the task up to an unimportant overall phase). Therefore, the theorem allows cloning of states with these phases.

Proof. First note that without loss of generality one can always assume that the first state $|\psi_e\rangle^{AB}$ is already in Schmidt form,

$$|\psi_e\rangle^{AB} = \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B, \tag{4.39}$$

since this can be done by a local unitary map $U^{Aa} \otimes V^{Bb}$. Therefore, the operators ψ_e and ψ_g obtained by map-state duality can be assumed to have the form

$$\psi_e = \begin{pmatrix} \sqrt{\lambda} & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \tag{4.40}$$

$$\psi_g = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}, \tag{4.41}$$

where λ is the largest Schmidt coefficient of $|\psi_e\rangle^{AB}$ and a_{ij} are complex numbers with $\sum |a_{ij}|^2 = 1$, which is equivalent to the requirement that $|\psi_g\rangle$ be normalized.

Orthogonality between these two states implies that

$$0 = \sqrt{\lambda}a_{00} + \sqrt{1-\lambda}a_{11}. \tag{4.42}$$

Since the only group of order 2 is cyclic with elements e, g and $g^2 = e$, we have from Theorem 4.3 that $(T_g^{(m)})^2 = SL(g)^2 S^{-1} = I$. Thus, we require

$$(\psi_g \psi_e^{-1})^2 = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\vartheta} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\vartheta} \end{pmatrix}, \tag{4.43}$$

where the factor of $\mathrm{e}^{\mathrm{i}\vartheta}$ arises from the phases that appear in the definition of $T_g^{(m)}$, see (4.22). Thus, (4.43) implies

$$\frac{a_{00}^2}{\lambda} = \frac{a_{11}^2}{1-\lambda} = \mathrm{e}^{\mathrm{i}\vartheta} - \frac{a_{01}a_{10}}{\sqrt{\lambda(1-\lambda)}}, \tag{4.44}$$

and either (i) $a_{00}\sqrt{1-\lambda} = -a_{11}\sqrt{\lambda}$; or (ii) $a_{01} = 0 = a_{10}$. The condition that ψ_g be normalized in the latter case (ii), along with (4.42) and (4.44), can only be satisfied if $\lambda = 1/2$, a case we are not considering here. The former case (i) along with (4.42) implies that $a_{00} = 0 = a_{11}$ (again, assuming $\lambda \neq 1/2$). This concludes the proof, since it implies that $|\psi_g\rangle^{AB}$ has to have either the form (4.37) or the form (4.38), up to an unimportant global phase. □

Now one can immediately see that one of the families of states considered in [CKRR07], of the form $|\psi_e\rangle = \sqrt{\lambda}|0\rangle^A|0\rangle^B + \sqrt{1-\lambda}|1\rangle^A|1\rangle^B$ and $|\psi_g\rangle = \sqrt{1-\lambda}|0\rangle^A|0\rangle^B - \sqrt{\lambda}|1\rangle^A|1\rangle^B$ cannot be locally cloned with a blank state of Schmidt rank 2, unless they are maximally entangled, case already studied in [ACP04].

4.4 Local cloning of group-shifted states: explicit protocol using a maximally entangled blank state

Consider now a set of group-shifted partially entangled states $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$, where the dimension of both Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ is equal to D,

$$|\psi_f\rangle^{AB} = \sum_{g\in G} \sqrt{\lambda_g}|g\rangle^A|fg\rangle^B, \tag{4.45}$$

and we remind the reader that throughout this section we restrict to the $|G| = D$ case (see Appendix 4.B for the $|G| < D$ case).

In the following we present a protocol that locally clones $\mathcal{S}$ using a maximally entangled blank state of Schmidt rank D. Our protocol, which works for any group G, is a direct generalization of the one presented for the special case of a cyclic group in [KE06].

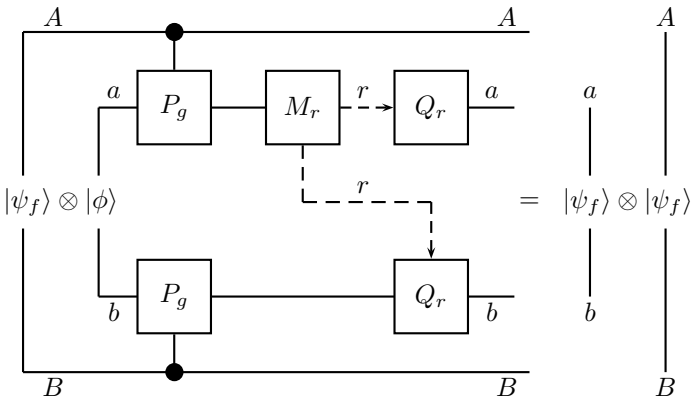

Figure 4.1: Circuit diagram for the local cloning of group-shifted states with a maximally entangled blank state. There is no need to perform the measurement M_r and the corrections Q_r whenever the states to be cloned are maximally entangled.

Theorem 4.8 (Group shifted states)**.** *Let $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of group-shifted full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$ as defined by* (4.45)*. The local cloning of $\mathcal{S}$ is always possible using a maximally entangled blank state $|\phi\rangle^{ab}$ of Schmidt rank D.*

Proof. Without loss of generality the maximally entangled blank state can be written as

$$|\phi\rangle^{ab} = \frac{1}{\sqrt{D}} \sum_{h\in G} |h\rangle^a |h\rangle^b. \tag{4.46}$$

The local cloning protocol is summarized below and the quantum circuit is displayed in Fig. 4.1.

1. Starting with $|\psi_f\rangle^{AB} \otimes |\phi\rangle^{ab}$, both Alice and Bob apply the "controlled-group" unitary

$$\sum_{g\in G} |g\rangle\langle g| \otimes P_g, \quad \text{with } P_g = \sum_{h\in G} |gh\rangle\langle h|, \tag{4.47}$$

where the permutation P_g acts on system a (b) and is controlled by system A (B), to obtain

$$\begin{aligned} &\sum_{g\in G} \sqrt{\lambda_g} |g\rangle^A |fg\rangle^B \frac{1}{\sqrt{D}} \sum_{h\in G} |gh\rangle^a |fgh\rangle^b \\ &= \sum_{g\in G} \sqrt{\lambda_g} |g\rangle^A |fg\rangle^B \frac{1}{\sqrt{D}} \sum_{h\in G} |h\rangle^a |fh\rangle^b. \end{aligned} \tag{4.48}$$

2. Next Alice performs a generalized measurement on system a with Kraus operators

$$M_r = \sum_{h\in G} \sqrt{\lambda_{hr}} |h\rangle\langle h|, \quad \sum_{r\in G} {M_r}^\dagger M_r = I, \tag{4.49}$$

and communicates the result r to Bob. Conditioned on the result r, the output state is

$$\sum_{g\in G} \sqrt{\lambda_g} |g\rangle^A |fg\rangle^B \sum_{h\in G} \sqrt{\lambda_{hr}} |h\rangle^a |fh\rangle^b. \tag{4.50}$$

3. Both Alice and Bob apply the unitary correction

$$Q_r = \sum_{h\in G} |hr\rangle \langle h| \tag{4.51}$$

on systems a and b, respectively, to obtain

$$\begin{aligned}
&\sum_{g\in G} \sqrt{\lambda_g}|g\rangle^A|fg\rangle^B \sum_{h\in G} \sqrt{\lambda_{hr}}|hr\rangle^a|fhr\rangle^b \\
&= \sum_{g\in G} \sqrt{\lambda_g}|g\rangle^A|fg\rangle^B \sum_{h\in G} \sqrt{\lambda_h}|h\rangle^a|fh\rangle^b \\
&= |\psi_f\rangle^{AB} \otimes |\psi_f\rangle^{ab},
\end{aligned} \tag{4.52}$$

which is the desired output.

□

Note that from symmetry considerations states of the form $\sum_{g\in G} \sqrt{\lambda_g}|fg\rangle^A|g\rangle^B$ (with the term fg appearing now on Alice's side instead of Bob's side) can also be locally-cloned, by interchanging the roles of Alice and Bob in the protocol, e.g. performing the measurement M_r on system b instead of a, then sending the result back to a. Therefore in the following, when discussing group-shifted states, we will restrict to the states of the form (4.45).

4.5 Local cloning of group-shifted states: minimum entanglement of the blank

Here again, we restrict for simplicity to the $|G| = D$ case, and discuss the extension of the results for $|G| < D$ in Appendix 4.B.

4.5.1 Necessary conditions for arbitrary D

We now turn our attention to the task of characterizing the blank state, which essentially amounts to determining the amount of entanglement it must have in order for the local cloning to be possible. We first give a very general lower bound as,

Theorem 4.9 (Minimum entanglement of the blank)**.** *Let $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab} \in \mathcal{H}_a \otimes \mathcal{H}_b$ is possible by a separable operation, then it must be that*

$$Ent(|\phi\rangle^{ab}) \geqslant \max_{f\in G} Ent(|\psi_f\rangle^{AB}), \tag{4.53}$$

where $Ent(\cdot)$ denotes any pure-state entanglement measure.

Proof. We recently proved in [GG08] that any pure state entanglement monotone is non-increasing on average under the general class of separable operations. The theorem follows directly, since otherwise the local cloning machine increases entanglement across the Aa/Bb cut. □

Providing a more detailed lower bound appears to be difficult in general, but turns out to be possible in the special case of group-shifted states.

Consider again the set of D group-shifted entangled states (4.45), and allow for arbitrary phases, $\vartheta_{f,g}$,

$$|\psi_f\rangle^{AB} = \sum_{g\in G} \sqrt{\lambda_g} \mathrm{e}^{\mathrm{i}\vartheta_{f,g}} |g\rangle^A|fg\rangle^B. \tag{4.54}$$

Without loss of generality, the blank state $|\phi\rangle^{ab}$ can be written as

$$|\phi\rangle^{ab} = \sum_{h\in G} \sqrt{\gamma_h}|h\rangle^a|h\rangle^b, \tag{4.55}$$

where γ_h are its Schmidt coefficients, $\sum_{h\in G}\gamma_h = 1$.

All states in $\mathcal{S}$ have the same Schmidt coefficients, and hence the same entanglement. As shown above, the local cloning of the above set of states is possible using a maximally entangled blank state when all phases $\mathrm{e}^{\mathrm{i}\vartheta_{f,g}}$ are chosen to be 1, but it is not yet known if one can accomplish this task using less entanglement. One might hope that the local cloning of $\mathcal{S}$ is possible using a blank state having the same entanglement as each of the states in $\mathcal{S}$, which could be regarded as an "optimal" local cloning. However we prove below that such an optimal local cloning is impossible with these states. Indeed we find a sizeable gap between the entanglement needed in the blank state and the entanglement of the states of $\mathcal{S}$. For $D = 2$ and $D = 3$, we prove that a maximally entangled blank state is *always* necessary.

In the rest of this section we will use the *rearrangement inequality* (see Chap. X of [HLP99]), which states that

$$x_n y_1 + \cdots + x_1 y_n \leqslant x_{\sigma(1)} y_1 + \cdots + x_{\sigma(n)} y_n \leqslant x_1 y_1 + \cdots + x_n y_n \tag{4.56}$$

for every choice of real numbers $x_1 \leqslant \cdots \leqslant x_n$ and $y_1 \leqslant \cdots \leqslant y_n$ and every permutation $x_{\sigma(1)}, \ldots, x_{\sigma(n)}$ of $x_1, \ldots, x_n$.

The following Lemma is the most important technical result of this section (note that in the statement of this result, we will use $\overline{g}$ for inverses g^{-1} of elements in the group G, which will make the notation somewhat more readable).

Lemma 4.10 (Majorization conditions)**.** *Let $\mathcal{S} = \{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of D group-shifted full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A \otimes \mathcal{H}_B$ as defined by* (4.54) *and considered to be not maximally entangled. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab}$ is possible by a separable operation, then*

i) The majorization condition,

$$\vec{\alpha} \prec \vec{\beta}, \tag{4.57}$$

must hold. Here, $\vec{\alpha}$ and $\vec{\beta}$ are vectors with D^2 components indexed by elements $g, h \in G$,

$$\alpha_{g,h} = \gamma_h \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}, \quad \beta_{g,h} = \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}\lambda_{fh}, \tag{4.58}$$

and $\{\mu_f\}_{f\in G}$ is an arbitrary set of non-negative real coefficients that satisfy $\sum_f \mu_f = 1$.

ii) The smallest Schmidt coefficient $\gamma_{\min}$ of the blank state has to satisfy

$$\gamma_{\min} \geqslant \max_{\{\mu_f\}} \frac{\min_{g,h\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}\lambda_{fh}}{\min_{g\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}}. \tag{4.59}$$

iii) In particular, a good choice of $\{\mu_f\}$ is given by

$$\mu_f = \frac{\eta}{\lambda_{\overline{f}}}, \quad \text{with } \eta^{-1} = \sum_{g\in G} 1/\lambda_g, \tag{4.60}$$

for which (4.59) *becomes*

$$\gamma_{\min} \geqslant \frac{1}{D} \min_{g,h\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg}\lambda_{fh}. \tag{4.61}$$

The majorization relation (4.57) restricts the possible allowed Schmidt coefficients for the blank state and can easily be checked numerically, but an analytic expression is difficult to find, since there is no simple way of ordering (4.58). That is why parts ii) and iii) of the Lemma have their importance, since they focus only on the smallest Schmidt coefficient of the blank state. In particular, the bound iii) is crucial in deriving the necessity of a maximally entangled blank state for the local cloning of qubit and group-shifted qutrit states.

The proof of the Lemma is rather technical and is presented in Appendix 4.A.2. However, the main idea of the proof consists of adding an ancillary system $\mathcal{H}_E$ of dimension D on Alice's side and then considering a superposition $\sum_{f\in G}\sqrt{\mu_f}|\psi_f\rangle^{AB}\otimes|\phi\rangle^{ab}\otimes|f\rangle^E$, that will be mapped by the deterministic separable operation to an ensemble $\{p_m,|\Psi_{m,\text{out}}\rangle^{AaBbE}\}$, with $|\Psi_{m,\text{out}}\rangle^{AaBbE}=\sum_{f\in G}\mathrm{e}^{\mathrm{i}\varphi_{mf}}\sqrt{\mu_f}|\psi_f\rangle^{AB}\otimes|\psi_f\rangle^{ab}\otimes|f\rangle^E$, and we have used the fact discovered above that $p_{mf}=p_m$, independent of f. The average Schmidt vector of the output ensemble over the AaE/Bb cut has to majorize the input Schmidt vector, see [GG08], and this yields i). Parts ii) and iii) are direct implications of i).

4.5.2 Qubits and Qutrits

When $D=2$ or $D=3$, one can easily show that the minimum in (4.61) is exactly one, and therefore

Theorem 4.11 (Necessity of maximally entangled blank)**.** *The following must hold.*

i) A maximally entangled state of Schmidt rank 2 is the minimum required resource for the local cloning of 2 entangled qubit states.

ii) A maximally entangled state of Schmidt rank 3 is the minimum required resource for the local cloning of 3 group-shifted entangled qutrit states.

The proof of both i) and ii) follows easily from Lemma 4.10, iii), by applying the rearrangement inequality to (4.61), and is presented in Appendix 4.A.3.

When $D=2$, or when $D=3$ and all phases $\mathrm{e}^{\mathrm{i}\vartheta_{f,g}}=1$, an explicit protocol for cloning these states exists [KE06] (alternatively, see the proof of our Theorem 4.8), and therefore Theorem 4.11 becomes a necessary and sufficient condition for the local cloning of such states. In particular, together with Theorem 4.7, it provides a complete solution to the problem of local cloning when $D=2$.

4.5.3 $D>3$, finite gap in the necessary entanglement

For $D>3$, preliminary numerical studies indicate that the minimum (4.61) in Lemma 4.10, iii) is often equal to one, with few exceptions. It might be the case that a better choice of $\{\mu_f\}$ in (4.59) of Lemma 4.10, ii) may provide the $1/D$ lower bound, but we were unable to prove this.

However, for any set of group-shifted states, we can prove that there is a rather sizeable gap between the entanglement needed in the blank state and the entanglement of the states of $\mathcal{S}$, as stated by the following theorem.

Theorem 4.12 (Finite gap)**.** *Let $\mathcal{S}=\{|\psi_f\rangle^{AB}\}_{f\in G}$ be a set of D group-shifted full Schmidt rank bipartite orthogonal entangled states on $\mathcal{H}_A\otimes\mathcal{H}_B$ as defined by* (4.54) *and considered to be not maximally entangled. If the local cloning of $\mathcal{S}$ using a blank state $|\phi\rangle^{ab}$ is possible by a separable operation, then the entanglement of the blank state has to be strictly greater that the entanglement of the states in $\mathcal{S}$, often by a wide margin. Specifically,*

$$E(|\phi\rangle^{ab})\geqslant H(\{q_r\})>E(|\psi_f\rangle^{AB}),\forall f\in G, \tag{4.62}$$

where $E(\cdot)$ denotes the entropy of entanglement and $H(\{q_r\})$ is the Shannon entropy of the probability distribution $\{q_r\}$, $q_r:=\sum_{f\in G}\lambda_f\lambda_{fr}$, $\sum_{r\in G}q_r=1$.

The proof follows by setting $\mu_f=1/D$ in Lemma 4.10, i), but is rather long and is presented in Appendix 4.A.4.

4.6 Conclusion and open questions

We have investigated the problem of local cloning of a set $\mathcal{S}$ of bipartite $D \times D$ entangled states by separable operations, at least one of which is full Schmidt rank. We proved that all states in $\mathcal{S}$ must be full rank and that the maximal set of clonable states must be generated by a finite group G of order N, the number of states in this maximal set, and then we showed that N has to divide D exactly. We further proved that all states in $\mathcal{S}$ must be equally entangled with respect to the G-concurrence measure, and this implied that any two states in $\mathcal{S}$ must either share the same set of Schmidt coefficients or otherwise be incomparable under majorization.

We have completely solved two important problems in local cloning. For $D = 2$ (entangled qubits), we proved that no more than two states can be locally cloned, and that these states must be locally-shifted. We showed that a two-qubit maximally entangled state is a necessary and sufficient resource for such a cloning. In addition, we provided necessary and sufficient conditions when the states are maximally entangled, valid for any dimension D, showing that the states must be group-shifted, and then we also provided an LOCC protocol that clones such a set of states.

We have studied in detail the local cloning of partially entangled group-shifted states and provided an explicit protocol for local cloning of such states with a maximally entangled resource. For $D = 3$ (entangled qutrits) we showed that a maximally entangled blank state is also necessary and sufficient, whereas for $D > 3$ we proved that the blank state has to be strictly more entangled than any state in $\mathcal{S}$, often by a sizeable amount.

The necessary form of the clonable states for $D > 2$ remains an open problem. One might guess that the states have to be of a group-shifted form, but a proof of such a claim is not presently available. Although we proved the necessity of a maximally entangled resource for the $D = 2$ case and for group-shifted states in the $D = 3$ case, in higher dimensions it is still not clear if a maximally entangled state of Schmidt rank D is always necessary. Finally it would be of interest to investigate the local cloning of less than full Schmidt rank states, a problem that is likely to bring in additional complications, such as the possibility of first distinguishing amongst the states in $\mathcal{S}$ while preserving the states intact [Coh07], and then once the state is known, the cloning becomes straightforward with a blank state having Schmidt coefficients that are majorized by those of each of the states in $\mathcal{S}$ [Nie99, GG08].

4.A Mathematical proofs

4.A.1 Proof of Lemma 4.5

Consider the singular value decomposition of S, $S = V\mathcal{D}U$ with $\mathcal{D}$ diagonal and positive definite, and V and U unitary operators. Using this expression for S in $T_f = SL(f)S^{-1}$ shows that

$$V^\dagger T_f V = \mathcal{D}(UL(f)U^\dagger)\mathcal{D}^{-1}, \tag{4.63}$$

or with $\tilde{T}_f = V^\dagger T_f V$ and $\tilde{L}(f) = UL(f)U^\dagger$,

$$\tilde{T}_f \mathcal{D} = \mathcal{D}\tilde{L}(f). \tag{4.64}$$

Since $\tilde{T}_f$ and $\tilde{L}(f)$ are both unitary, it is not difficult to see from this that each commutes with $\mathcal{D}^\dagger\mathcal{D} = \mathcal{D}^2$. That is,

$$\begin{aligned} \mathcal{D}_i^2[\tilde{T}_f]_{ij} &= [\tilde{T}_f]_{ij}\mathcal{D}_j^2 \\ \mathcal{D}_i^2[\tilde{L}(f)]_{ij} &= [\tilde{L}(f)]_{ij}\mathcal{D}_j^2, \end{aligned} \tag{4.65}$$

from which we conclude that when $\mathcal{D}_i \neq \mathcal{D}_j$, $[\tilde{T}_f]_{ij} = 0 = [\tilde{L}(f)]_{ij}$. By a judicious choice of U and V, we may arrange for $\mathcal{D}$ to be a direct sum of scalar matrices (some may be one-dimensional).

That is, $\mathcal{D} = \oplus_\nu \alpha_\nu I_\nu$, and then we see that T_f and $L(f)$ share the same block-diagonal structure, with blocks corresponding to this direct sum decomposition of $\mathcal{D}$.

We also have directly from (4.64) that

$$[\tilde{T}_f]_{ij}\mathcal{D}_j = \mathcal{D}_i[\tilde{L}(f)]_{ij}. \tag{4.66}$$

Therefore, when $\mathcal{D}_j = \mathcal{D}_i$, $[\tilde{T}_f]_{ij} = [\tilde{L}(f)]_{ij}$, and we see that the blocks of $\tilde{T}_f$ are identical to those of $\tilde{L}(f)$. In other words, we have shown that $\tilde{T}_f = \tilde{L}(f)$ or equivalently, $T_f = WL(f)W^\dagger$ with $W = VU$, completing the proof.

4.A.2 Proof of Lemma 4.10

Proof of i) Let us introduce an ancillary system $\mathcal{H}_E$ of dimension D on Alice's side and construct the superposition

$$|\Psi_{\rm in}\rangle^{ABabE} := \sum_{f\in G} \sqrt{\mu_f}|\psi_f\rangle^{AB} \otimes |\phi\rangle^{ab} \otimes |f\rangle^E, \tag{4.67}$$

with $\{\mu_f\}_{f\in G}$ an arbitrary set of non-negative real coefficients that satisfy $\sum_f \mu_f = 1$. The proof is based on the fact that if $|\psi_f\rangle^{AB} \otimes |\phi\rangle^{ab}$ is deterministically mapped to $\mathrm{e}^{\mathrm{i}\varphi_{mf}}|\psi_f\rangle^{AB} \otimes |\psi_f\rangle^{ab}$ (see (4.11)), then $|\Psi_{\rm in}\rangle^{ABabE}$ will be deterministically mapped to an ensemble $\{p_m, |\Psi_{m,\rm out}\rangle^{AaBbE}\}$, where

$$|\Psi_{m,\rm out}\rangle^{AaBbE} = \sum_{f\in G} \mathrm{e}^{\mathrm{i}\varphi_{mf}}\sqrt{\mu_f}|\psi_f\rangle^{AB} \otimes |\psi_f\rangle^{ab} \otimes |f\rangle^E. \tag{4.68}$$

Note that this conclusion rests crucially on the fact, discovered in the main text, that $p_{mf} = p_m$, independent of f.

Let us now write $|\Psi_{\rm in}\rangle^{ABabE}$ in Schmidt form over the AaE/Bb cut. One has (again we use $\overline{f} = f^{-1}$)

$$\begin{aligned}
|\Psi_{\rm in}\rangle^{ABabE} &= \sum_{f\in G}\sqrt{\mu_f}\left(\sum_{g,h\in G}\mathrm{e}^{\mathrm{i}\vartheta_{f,g}}\sqrt{\lambda_g\gamma_h}\,|g\rangle^A|fg\rangle^B|h\rangle^a|h\rangle^b\right)|f\rangle^E \\
&= \sum_{f,g,h\in G}\mathrm{e}^{\mathrm{i}\vartheta_{f,g}}\sqrt{\mu_f\lambda_g\gamma_h}\,|g\rangle^A|h\rangle^a|f\rangle^E \otimes |fg\rangle^B|h\rangle^b \\
&= \sum_{g,h\in G}\left(\sum_{f\in G}\mathrm{e}^{\mathrm{i}\vartheta_{f,\overline{f}g}}\sqrt{\mu_f\lambda_{\overline{f}g}\gamma_h}|\overline{f}g\rangle^A|f\rangle^E\right)|h\rangle^a \otimes |g\rangle^B|h\rangle^b \\
&= \sum_{g,h\in G}\left(\sum_{f\in G}\mathrm{e}^{\mathrm{i}\vartheta_{\overline{f},fg}}\sqrt{\mu_{\overline{f}}\lambda_{fg}\gamma_h}|fg\rangle^A|\overline{f}\rangle^E\right)|h\rangle^a \otimes |g\rangle^B|h\rangle^b,
\end{aligned} \tag{4.69}$$

where we used the group property of G and replaced g by $\overline{f}g$ and summation over f by summation over $\overline{f}$ where necessary. The states on the AaE system are orthogonal for different pairs of g, h, and therefore (4.69) represents a Schmidt decomposition, with Schmidt coefficients $\alpha_{g,h}$ given by the squared norm of the states on the AaE system,

$$\alpha_{g,h} = \gamma_h \sum_{f\in G}\mu_{\overline{f}}\lambda_{fg}. \tag{4.70}$$

A similar calculation yields for the Schmidt coefficients $\beta_{g,h}$ of $|\Psi_{m,\rm out}\rangle^{ABabE}$ the expression

$$\beta_{g,h} = \sum_{f\in G}\mu_{\overline{f}}\lambda_{fg}\lambda_{fh}, \tag{4.71}$$

independent of m, which means that the average Schmidt vector of the output ensemble under the Aa/BbE cut is the same as the Schmidt vector of an individual state $|\Psi_{m,\text{out}}\rangle^{ABabE}$.

We have proven in [GG08] that the average Schmidt vector of the output ensemble produced by a separable operation acting on a pure state has to majorize the input Schmidt vector, and this concludes i).

Proof of ii) The proof follows as a direct consequence of i). A particular majorization inequality imposed by Lemma 4.10 i) requires that the smallest Schmidt coefficients $\alpha_{\min}$ and $\beta_{\min}$ have to satisfy

$$\alpha_{\min} \geqslant \beta_{\min}, \tag{4.72}$$

where α and β were defined in (4.70) and (4.71), respectively. This is equivalent to

$$\gamma_{\min} \geqslant \frac{\min_{g,h\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}\lambda_{fh}}{\min_{g\in G} \sum_{f\in G} \mu_{\overline{f}} \lambda_{fg}}. \tag{4.73}$$

The above equation must hold regardless of which set of $\{\mu_f\}$ was chosen, hence taking the maximum over all possible sets $\{\mu_f\}$ concludes the proof of ii).

Proof of iii) Inserting the expression (4.60) for $\{\mu_f\}$ in (4.73) yields

$$\gamma_{\min} \geqslant \frac{\min_{g,h\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg}\lambda_{fh}}{\min_{g\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg}} \tag{4.74}$$

$$= \frac{1}{D} \min_{g,h\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg}\lambda_{fh}, \tag{4.75}$$

where (4.75) follows from applying the rearrangement inequality to the denominator in (4.74), which in this case reads as

$$\min_{g\in G} \sum_{f\in G} \frac{1}{\lambda_f} \lambda_{fg} = \sum_{f\in G} \frac{1}{\lambda_f} \lambda_f = D. \tag{4.76}$$

4.A.3 Proof of Theorem 4.11

Proof of i) In this case the group G is the cyclic group of order 2, and we identify its group elements by $\{0, 1\}$. We proved in Theorem 4.7 that the qubit states have to be locally shifted. The minimum in (4.61) of Lemma 4.10, iii) becomes explicitly a minimum over 4 quantities that correspond to all possible pairings of g, h; a straightforward calculation shows that 3 out of these 4 quantities are equal to 1, except for $g = h = 1$, in which case the sum in (4.75) equals $\lambda_1^2/\lambda_0 + \lambda_0^2/\lambda_1$. Order the λ's such that $\lambda_0 \geqslant \lambda_1$ and note that

$$\frac{1}{\lambda_0} \leqslant \frac{1}{\lambda_1} \text{ and} \tag{4.77}$$

$$\lambda_1^2 \leqslant \lambda_0^2. \tag{4.78}$$

From the rearrangement inequality applied to (4.77) and (4.78) it follows that

$$\frac{\lambda_1^2}{\lambda_0} + \frac{\lambda_0^2}{\lambda_1} \geqslant \frac{\lambda_0^2}{\lambda_0} + \frac{\lambda_1^2}{\lambda_1} = 1, \tag{4.79}$$

and hence the minimum in case i) equals 1.

Proof of ii) Now the group G is isomorphic to the cyclic group of order 3 and again we identify its elements by $\{0, 1, 2\}$. We order the λ's such that $\lambda_0 \geqslant \lambda_1 \geqslant \lambda_2$. The minimum in (4.75) is now taken over 9 possible pairs g, h. Again straightforward algebra shows that most expressions sum up to 1, except for the following three cases for which we show that the sum exceeds 1.

1. $g = h = 1$, for which the sum in (4.75) equals $\lambda_1^2/\lambda_0 + \lambda_2^2/\lambda_1 + \lambda_0^2/\lambda_2$;
2. $g = h = 2$, for which the sum in (4.75) equals $\lambda_2^2/\lambda_0 + \lambda_0^2/\lambda_1 + \lambda_1^2/\lambda_2$;
3. $g = 1, h = 2$ or $g = 2, h = 1$, for which the sum in (4.75) equals $\lambda_1\lambda_2/\lambda_0 + \lambda_2\lambda_0/\lambda_1 + \lambda_0\lambda_1/\lambda_2$.

Note first that

$$\frac{1}{\lambda_0} \leqslant \frac{1}{\lambda_1} \leqslant \frac{1}{\lambda_2} \tag{4.80}$$

$$\lambda_2{}^2 \leqslant \lambda_1{}^2 \leqslant \lambda_0{}^2 \text{ and} \tag{4.81}$$

$$\lambda_1\lambda_2 \leqslant \lambda_2\lambda_0 \leqslant \lambda_0\lambda_1. \tag{4.82}$$

From the rearrangement inequality applied to (4.80) and (4.81) it follows that

$$\begin{aligned} &\frac{1}{\lambda_0}\lambda_1^2 + \frac{1}{\lambda_1}\lambda_2^2 + \frac{1}{\lambda_2}\lambda_0^2 \geqslant \\ &\geqslant \frac{1}{\lambda_0}\lambda_0^2 + \frac{1}{\lambda_1}\lambda_1^2 + \frac{1}{\lambda_2}\lambda_2^2 = 1, \end{aligned} \tag{4.83}$$

which proves case 1, and

$$\begin{aligned} &\frac{1}{\lambda_0}\lambda_2^2 + \frac{1}{\lambda_1}\lambda_0^2 + \frac{1}{\lambda_2}\lambda_1^2 \geqslant \\ &\geqslant \frac{1}{\lambda_0}\lambda_0^2 + \frac{1}{\lambda_1}\lambda_1^2 + \frac{1}{\lambda_2}\lambda_2^2 = 1, \end{aligned} \tag{4.84}$$

which proves case 2.

Next apply the rearrangement inequality to (4.80) and (4.82) to get

$$\begin{aligned} &\frac{1}{\lambda_0}(\lambda_1\lambda_2) + \frac{1}{\lambda_1}(\lambda_2\lambda_0) + \frac{1}{\lambda_2}(\lambda_0\lambda_1) \\ &\geqslant \frac{1}{\lambda_0}\lambda_0\lambda_1 + \frac{1}{\lambda_1}\lambda_1\lambda_2 + \frac{1}{\lambda_2}\lambda_0\lambda_2 = 1 \end{aligned} \tag{4.85}$$

and this proves case 3.

4.A.4 Proof of Theorem 4.12

By setting $\mu_f = 1/D$ in Lemma 4.10, i), for all $f \in G$, the majorization relation (4.57) reads as

$$\frac{1}{D}\vec{\gamma} \times \vec{1} \prec \vec{\beta}, \tag{4.86}$$

where $(1/D)\vec{\gamma} \times \vec{1}$ represents a D^2 component vector with components γ_h/D, each component repeated D times; here $\vec{\gamma}$ is the Schmidt vector of the blank state $|\phi\rangle^{ab}$. The D^2 components $\beta_{g,h}$ of $\vec{\beta}$ are given by

$$\beta_{g,h} = \frac{1}{D}\sum_{f\in G} \lambda_{fg}\lambda_{fh} = \frac{1}{D}\sum_{f\in G} \lambda_f \lambda_{f\overline{g}h}. \tag{4.87}$$

Note that it is also the case that β has D components each repeated D times, so the majorization relation (4.86) implies a majorization relation between 2 D-component vectors

$$\vec{\gamma} \prec \vec{q}, \tag{4.88}$$

where the r-th component of $\vec{q}$ is given by

$$q_r := D \cdot \beta_{g,h}|_{\overline{g}h=r} = \sum_{f\in G} \lambda_f \lambda_{fr}. \tag{4.89}$$

Note that both $\vec{\gamma}$ and $\vec{q}$ are normalized probability vectors. Since the Shannon entropy is a Schur-concave function, (4.88) implies at once that

$$E(|\phi\rangle^{ab}) \geqslant H(\{q_r\}). \tag{4.90}$$

We now show that the second inequality in (4.62) is strict. First we will prove that the ordered vector of probabilities $\vec{q}^{\downarrow}$ with components defined in (4.89) and decreasing magnitudes of entries down its column, is majorized by $\vec{\lambda}^{\downarrow}$, the ordered vector of the λ_f,

$$\vec{q}^{\downarrow} \prec \vec{\lambda}^{\downarrow}. \tag{4.91}$$

Since the Shannon entropy is not just Schur-concave, but strictly Schur-concave, this will imply at once that

$$H(\{q_r\}) \geqslant H(\{\lambda_f\}) = E(|\psi_f\rangle^{AB}),\ \forall f \in G, \tag{4.92}$$

with equality if and only if $\vec{q}^{\downarrow}$ equals $\vec{\lambda}^{\downarrow}$ (or, equivalently, if and only if the unordered vector $\vec{q}$ is the same as $\vec{\lambda}$ up to a permutation). One can see that $\vec{q}$ is not a permutation of $\vec{\lambda}$ unless all λ's are equal, case that we exclude. Hence, once we show the majorization condition (4.91) holds, the proof will be complete.

We will actually show that $\vec{\lambda}^{\downarrow}$ majorizes every vector $\vec{q}$ of the q_r's no matter how $\vec{q}$ is ordered. Denote by S_n, with $|S_n| = n$ and $n = 1, \cdots, D-1$, the subset consisting of those elements $f \in G$ such that λ_f is one of the largest n of the λ's. Then, we need to show that for each n,

$$\sum_{g\in S_n} \lambda_g \geqslant \sum_{g\in S_n} q_{\sigma(g)} = \sum_{g\in S_n} \sum_{f\in G} \lambda_f \lambda_{f\sigma(g)}, \tag{4.93}$$

where σ is an arbitrary permutation of the group elements. Since $\sum_f \lambda_f = 1$, this is equivalent to

$$\sum_{f\in G} \lambda_f \left[\sum_{g\in S_n} \lambda_g - \sum_{g\in S_n} \lambda_{f\sigma(g)} \right] \geqslant 0. \tag{4.94}$$

However, given the way we have defined S_n, it is always true that the quantity in square brackets is non-negative. The reason is that the first term in this quantity is the sum of the n largest of the λ's. Therefore the second term, which is also a sum of n of the λ's, cannot possibly be greater than the first. In fact, it is clear that for general sets of Schmidt coefficients $\{\lambda_f\}$, the quantity in square brackets will not be particularly small, implying that the gap between the required entanglement of the blank state and the entanglement of the states in $\mathcal{S}$ will be sizable. This ends the proof.

4.B $|G| < D$ case

In the main body of the current chapter, we restricted our consideration to the $|G| = D$ case. All of our results remain valid also when $|G| < D$, with minor modifications. Briefly, when $|G| < D$, $T_f^{(m)}$ is a direct sum of $n_t = D/|G|$ copies of $L(f)$, and the following Theorems/Lemmas have to be modified accordingly.

Theorem 4.6.

Since Lemma 4.5 holds for any two unitary representations, it will hold when the regular representation $L(f)$ is replaced by a direct sum of a number of copies of $L(f)$. In this case, the maximally entangled group-shifted states (4.35) and (4.36) of Theorem 4.6 have the form

$$|\psi_f\rangle^{AB} = \frac{1}{\sqrt{D}} \sum_{n=1}^{n_t} \sum_{g\in G} |fg,n\rangle^A |g,n\rangle^B, \tag{4.95}$$

or

$$|\psi_f\rangle^{AB} = \frac{1}{\sqrt{D}} \sum_{n=1}^{n_t} \sum_{g\in G} |g,n\rangle^A |fg,n\rangle^B, \tag{4.96}$$

respectively. Here the states $\{|g,n\rangle\}_{g\in G, n=1,\ldots,n_t}$ are an orthonormal basis, $\langle g,n|h,m\rangle = \delta_{g,h}\delta_{n,m}$. The symbols $f,g \in G$ label the group elements and $m,n = 1,\ldots,n_t$ label the copies of the regular representation.

Theorem 4.8.

When the family of partially entangled group-shifted states (4.45) is replaced by

$$|\psi_f\rangle^{AB} = \sum_{n=1}^{n_t} \sum_{g\in G} \sqrt{\lambda_{g,n}} |g,n\rangle^A |fg,n\rangle^B \tag{4.97}$$

and the maximally entangled blank state (4.46) is modified to

$$|\phi\rangle^{ab} = \frac{1}{\sqrt{D}} \sum_{m=1}^{n_t} \sum_{h\in G} |h,m\rangle^a |h,m\rangle^b, \tag{4.98}$$

the local cloning protocol of Theorem 4.8 continues to work, provided that

1. The controlled-group unitary (4.47) is replaced by

$$\sum_{n=1}^{n_t} \sum_{g\in G} |g,n\rangle \langle g,n| \otimes P_g, \text{with}$$
$$P_g = \sum_{m=1}^{n_t} \sum_{h\in G} |gh,m\rangle \langle h,m| . \tag{4.99}$$

2. The measurement (4.49) Alice performs is changed to

$$M_r = \sum_{m=1}^{n_t} \frac{1}{(\sum_{k\in G} \lambda_{k,m})^{1/2}} \sum_{h\in G} \sqrt{\lambda_{hr,m}} |h,m\rangle \langle h,m| . \tag{4.100}$$

   where the factor involving the sum over k is needed to insure that this set of measurement operators corresponds to a complete measurement.

3. Finally the unitary correction (4.51) Alice and Bob perform is modified to

$$Q_r = \sum_{m=1}^{n_t} \sum_{h\in G} |hr,m\rangle \langle h,m| . \tag{4.101}$$

Lemma 4.10.

First the blank state has to be modified to

$$|\phi\rangle^{ab} = \frac{1}{\sqrt{D}} \sum_{m=1}^{n_t} \sum_{h\in G} \sqrt{\gamma_{h,m}} |h,m\rangle^a |h,m\rangle^b. \tag{4.102}$$

Next we follow the line of thought in Appendix 4.A.2. Even though there are only $|G| < D$ states in the clonable set $\mathcal{S}$, we still use a D dimensional ancillary system $\mathcal{H}_E$ on Alice's side, with a basis now given by $\{|f,n\rangle^E\}_{f\in G, n=1,\ldots,n_t}$. Restricting to an ancillary system of dimension $|G|$ leads to unnecessary complications, since the rearrangement inequality can no longer be applied in part ii) to obtain iii).

We consider again an input superposition

$$\sum_{n=1}^{n_t}\sum_{f\in G}\sqrt{\mu_{f,n}}|\psi_f\rangle^{AB}\otimes|\phi\rangle^{ab}\otimes|f,n\rangle^E \tag{4.103}$$

and look at the Schmidt vector of the output ensemble produced by the separable operation acting on (4.103), where $\{\mu_{f,n}\}$ is an arbitrary set of coefficients satisfying $\sum_{n=1}^{n_t}\sum_{f\in G}\mu_{f,s}=1$. We then have:

i) The majorization condition $\vec{\alpha}\prec\vec{\beta}$ corresponding to (4.57) holds, provided the vectors $\vec{\alpha}$ and $\vec{\beta}$ in (4.58) are redefined as

$$\begin{aligned}\alpha_{g,h}^{n,m}&=\gamma_{h,m}\sum_{s=1}^{n_t}\sum_{f\in G}\mu_{\overline{f},s}\lambda_{fg,n},\\ \beta_{g,h}^{n,m}&=\sum_{s=1}^{n_t}\sum_{f\in G}\mu_{\overline{f},s}\lambda_{fg,n}\lambda_{fh,m}.\end{aligned} \tag{4.104}$$

ii) The smallest Schmidt coefficient $\gamma_{\min}$ of the blank has to satisfy

$$\gamma_{\min}\geqslant\max_{\{\mu_{f,s}\}}\frac{\min_{m,n}\min_{g,h\in G}\sum_{s=1}^{n_t}\sum_{f\in G}\mu_{\overline{f},s}\lambda_{fg,n}\lambda_{fh,m}}{\min_n\min_{g\in G}\sum_{s=1}^{n_t}\sum_{f\in G}\mu_{\overline{f},s}\lambda_{fg,n}}. \tag{4.105}$$

iii) A good choice of $\{\mu_{f,s}\}$ is given by $\mu_{f,s}=1/\lambda_{\overline{f},s}$ (ignore the normalization, since $\mu_{f,s}$ appears both on the numerator and denominator of (4.105)). Then (4.105) becomes

$$\gamma_{\min}\geqslant\frac{1}{|D|}\min_{m,n}\min_{g,h\in G}\sum_{s=1}^{n_t}\sum_{f\in G}\frac{1}{\lambda_{\overline{f},s}}\lambda_{fg,n}\lambda_{fh,m}. \tag{4.106}$$

Theorem 4.12.

Theorem 4.12 still provides a finite gap between the entanglement needed in the blank state and the entanglement of group shifted states (4.97). The proof follows the same ideas as before, by setting $\mu_{f,s}=1/D$, for all $f\in G$ and $s=1,\ldots,n_t$ in the majorization relation of the "modified" Lemma 4.10,i) above.

5

Quantum error correcting codes using qudit graph states

5.1 Introduction

Quantum error correction is an important part of various schemes for quantum computation and quantum communication, and hence quantum error correcting codes, first introduced about a decade ago [Sho95, KL97, Ste96] have received a great deal of attention. For a detailed discussion see Ch. 10 of [NC00]. Most of the early work dealt with codes for qubits, with a Hilbert space of dimension $D = 2$, but qudit codes with $D > 2$ have also been studied [Rai99, AK01, SW01, Schb, Scha, GBR04, AKP]. They are of intrinsic interest and could turn out to be of some practical value.

Cluster or graph states, which were initially introduced in connection with measurement based or one-way quantum computing [RB01], are also quite useful for constructing quantum codes, as shown in [SW01, Schb, Scha] in a context in which both the encoding operation and the resulting encoded information are represented in terms of graph states. In the present chapter we follow [Scha] in focusing on qudits with general D, thought of as elements of the additive group $\mathbb{Z}_D$ of integers mod D. However, our strategy is somewhat different, in that we use graph states and an associated basis (graph basis) of the n-qudit Hilbert space in order to construct the coding subspace, while *not* concerning ourselves with the encoding process. This leads to a considerable simplification of the problem along with the possibility of treating nonadditive graph codes on exactly the same basis as additive or stabilizer codes. It also clarifies the relationship (within the context of graph codes as we define them) of degenerate and nondegenerate codes, though in this chapter we focus mainly on the latter. The approach used here was developed independently in [CSSZ09] and [YCO] for $D = 2$, and in [HTZ$^+$08] for $D > 2$; thus several of our results are similar to those reported in these references.

Following an introduction in Sec. 5.2 to Pauli operators, graph states, and the graph basis, as used in this chapter, the construction of graph codes is the topic of Sec. 5.3. In Sec. 5.3.1 we review the conditions for an $((n, K, \delta))_D$ code, where n is the number of carriers, K the number of codewords or dimension of the coding space, δ the distance of the code, and D the dimension of the Hilbert space of one qudit. We also consider the distinction between degenerate and nondegenerate codes. Our definition of graph codes follows in Sec. 5.3.2, and the techniques we use to find nondegenerate codes, which are the main focus of this chapter, are indicated in Sec. 5.3.3, while various results in terms of specific codes are the subject of Sec. 5.4.

In Sec. 5.4.2 we show how to construct graph codes with $\delta = 2$ that saturate the quantum Singleton (QS) bound for arbitrarily large n and D, except when n is odd and D is even, and we derive a simple sufficient condition for graphs to yield such codes. For n odd and $D = 2$ we have an alternative and somewhat simpler method of producing nonadditive codes of the same size found in

[SSW07]. For both $D = 2$ and $D = 3$ we have studied nondegenerate codes on sequences of cycle and wheel graphs, in Secs. 5.4.3 and 5.4.4. These include a number of cases which saturate the QS bound for $\delta = 2$ and 3, and others with $\delta = 3$ and 4 which are the largest possible additive codes for the given n, D, and δ. Section 5.4.4 contains results for a series of hypercube graphs with $n = 4$, 8, and 16, and in particular a $((16, 128, 4))_2$ additive code.

In Sec. 5.5 we show that what we call G-additive codes are stabilizer codes (hence "additive" in the sense usually employed in the literature), using a suitable generalization of the stabilizer formalism to general D. In this perspective the stabilizer is a dual representation of a code which is equally well represented by its codewords. The final Sec. 5.6 has a summary of our results and indicates directions in which they might be extended.

5.2 Pauli operators and graph states

5.2.1 Pauli operators

Let $\{|j\rangle\}$, $j = 0, 1, \ldots D-1$ be an orthonormal basis for the D-dimensional Hilbert space of a qudit, and define the unitary operators [1]

$$Z = \sum_{j=0}^{D-1} \omega^j |j\rangle\langle j|\,, \quad X = \sum_{j=0}^{D-1} |j\rangle\langle j \oplus 1|\,, \tag{5.1}$$

with $\oplus$ denoting addition mod D. They satisfy

$$Z^D = I = X^D, \quad XZ = \omega ZX, \quad \omega := \mathrm{e}^{2\pi \mathrm{i}/D}. \tag{5.2}$$

We shall refer to the collection of D^2 operators $\{X^\mu Z^\nu\}$, $\mu, \nu = 0, 1, \ldots, D-1$, as (generalized) *Pauli operators*, as they generalize the well known $I, X, Z, XZ\,(= -iY)$ for a qubit. Together they form the *Pauli basis* of the space of operators on a qudit.

For a collection of n qudits with a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \mathcal{H}_n$ we use subscripts to identify the corresponding Pauli operators: thus Z_l and X_l operate on the space $\mathcal{H}_l$ of qudit l. An operator of the form

$$P = \omega^\lambda X_1^{\mu_1} Z_1^{\nu_1} X_2^{\mu_2} Z_2^{\nu_2} \cdots X_n^{\mu_n} Z_n^{\nu_n}, \tag{5.3}$$

where λ, and μ_l and ν_l for $1 \le l \le n$, are integers in the range 0 to $D-1$, will be referred to as a *Pauli product*. If μ_l and ν_l are both 0, the operator on qudit l is the identity, and can safely be omitted from the right side of (5.3). The collection $\mathcal{Q}$ of all operators P of the form (5.3) with $\lambda = 0$, i.e., a prefactor of 1, forms an orthonormal basis of the space of operators on $\mathcal{H}$ with inner product $\langle A, B\rangle = D^{-n}\mathrm{Tr}(A^\dagger B)$; we call it the (generalized) *Pauli basis* $\mathcal{Q}$.

If P and Q are Pauli products, so is PQ, and hence the collection $\mathcal{P}$ of all operators of the form (5.3) for n fixed form a multiplicative group, the *Pauli group*. While $\mathcal{P}$ is not Abelian, it has the property that

$$PQ = \omega^\mu QP, \tag{5.4}$$

where μ is an integer that depends on P and Q. (When $D = 2$ and $\omega = -1$ it is customary to also include in the Pauli group operators of the form (5.3) multiplied by i. For our purposes this makes no difference.)

The *base* of an operator P of the form (5.3) is the collection of qudits, i.e., the subset of $\{1, 2, \ldots n\}$, on which the operator acts in a nontrivial manner, so it is not just the identity, which is to say those j for which either μ_j or ν_j or both are greater than 0. A general operator R can be expanded in the Pauli basis $\mathcal{Q}$, and its base is the union of the bases of the operators which are present (with nonzero coefficients) in the expansion. The *size* of an operator R is defined as

[1] See [HDM05] for a list of references to work that employs operators of this type.

the number of qudits in its base, i.e., the number on which it acts in a nontrivial fashion. For example, the base of $P = \omega^2 X_1^2 X_4 Z_4$ (assuming $D \geq 3$) is $\{1, 4\}$ and its size is 2; whereas the size of $R = X_1 + 0.5 X_2 Z_2^2 Z_3 + i X_4$ is 4.

For two distinct qudits l and m the *controlled-phase* operation C_{lm} on $\mathcal{H}_l \otimes \mathcal{H}_m$, generalizing the usual controlled-phase for qubits, is defined by

$$C_{lm} = \sum_{j=0}^{D-1} \sum_{k=0}^{D-1} \omega^{jk} |j\rangle\langle j| \otimes |k\rangle\langle k| = \sum_{j=0}^{D-1} |j\rangle\langle j| \otimes Z_m^j. \tag{5.5}$$

Of course, $C_{lm} = C_{ml}$, and it is easily checked that $(C_{lm})^D = I$. It follows from its definition that C_{lm} commutes with Z_l and Z_m, and thus with Z_p for any qudit p.

5.2.2 Graph states

Let $G = (V, E)$ be a graph with n vertices V, each corresponding to a qudit, and a collection E of undirected edges connecting pairs of distinct vertices (no self loops). Multiple edges are allowed, as in Fig.5.1 for the case of $D = 4$, as long as the multiplicity (weight) does not exceed $D - 1$, thus at most a single edge in the case of qubits. The lm element $\Gamma_{lm} = \Gamma_{ml}$ of the *adjacency matrix* Γ is the number of edges connecting vertex l with vertex m. The graph state

$$|G\rangle = \mathcal{U}|G^0\rangle = \mathcal{U}\left(|+\rangle^{\otimes n}\right), \tag{5.6}$$

is obtained by applying the unitary operator

$$\mathcal{U} = \prod_{\{l,m\} \in E} (C_{lm})^{\Gamma_{lm}}. \tag{5.7}$$

to the product state

$$|G^0\rangle := |+\rangle \otimes |+\rangle \otimes \cdots |+\rangle, \tag{5.8}$$

where

$$|+\rangle := D^{-1/2} \sum_{j=0}^{D-1} |j\rangle \tag{5.9}$$

is a normalized eigenstate of X, with eigenvalue 1. In (5.7) the product is over all distinct pairs of qudits, with $(C_{lm})^0 = I$ when l and m are not joined by an edge. Since the C_{lm} for different l and m commute with each other, and also with Z_p for any p, the order of the operators on the right side of (5.7) is unimportant.

Given the graph G we define the *graph basis* to be the set of D^n states

$$\begin{aligned} |\mathbf{a}\rangle &:= |a_1, a_2, \ldots, a_n\rangle = Z^{\mathbf{a}} |G\rangle \\ &= Z_1^{a_1} Z_2^{a_2} \cdots Z_n^{a_n} |G\rangle \end{aligned} \tag{5.10}$$

where $\mathbf{a} = (a_1, \ldots a_n)$ is an n-tuple of integers, each taking a value between 0 and $D - 1$. The original graph state $|G\rangle$ is $|0, 0, \ldots, 0\rangle$ in this notation. That this collection forms an orthonormal basis follows from the fact that the Z_p operators commute with the C_{lm} operators, so can be moved through the unitary $\mathcal{U}$ on the right side of (5.6). As the states $Z^\nu|+\rangle$, $0 \leq \nu \leq D - 1$, are an orthonormal basis for a single qudit, their products form an orthonormal basis for n qudits. Applying the unitary $\mathcal{U}$ to this basis yields the orthonormal graph basis. The n-tuple representation in (5.10) is convenient in that one can define

$$\begin{aligned} |\mathbf{a} \oplus \mathbf{b}\rangle &:= |a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n\rangle, \\ |j\mathbf{a}\rangle &:= |ja_1, ja_2, \ldots, ja_n\rangle, \end{aligned} \tag{5.11}$$

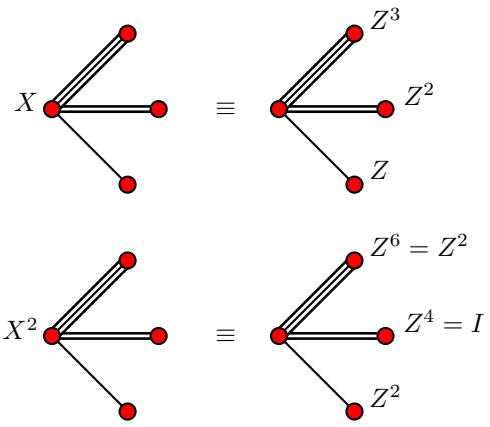

Figure 5.1: Action of X and X^2 on graph state ($D = 4$).

where j is an integer between 0 and $D-1$, and arithmetic operations are mod D.

One advantage of using the graph basis is that its elements are mapped to each other by a Pauli product (up to powers of ω), as can be seen by considering the action of Z_l or X_l on a single qudit. The result for Z_l follows at once from (5.10). And as shown in App. 5.A and illustrated in Fig. 5.1, the effect of applying X_l to $|G\rangle$ is the same as applying $(Z_m)^{\Gamma_{lm}}$ to each of the qudits corresponding to neighbors of l in the graph. Applying these two rules and keeping track of powers of ω resulting from interchanging X_l and Z_l, see (5.2), allows one to easily evaluate the action of any Pauli product on any $|\mathbf{a}\rangle$ in the graph basis.

5.3 Code construction

5.3.1 Preliminaries

Consider a quantum code corresponding to a K-dimensional subspace, with orthonormal basis $\{|\mathbf{c}_q\rangle\}$, of the Hilbert space $\mathcal{H}$ of n qudits. When the Knill-Laflamme [KL97] condition

$$\langle \mathbf{c}_q | \, Q | \mathbf{c}_r \rangle = f(Q)\delta_{qr} \tag{5.12}$$

is satisfied for all q and r between 0 and $K-1$, and every operator Q on $\mathcal{H}$ such that $1 \le \mathrm{size}(Q) < \delta$, but fails for some operators of size δ, the code is said to have *distance* δ, and is an $(\!(n, K, \delta)\!)_D$ code; the subscript is often omitted when $D = 2$. (See the definition of size in Sec. 5.2.1. The only operator of size 0 is a multiple of the identity, so (5.12) is trivially satisfied.) A code of distance δ allows the correction of any error involving at most $\lfloor (\delta-1)/2 \rfloor$ qudits, or an error on $\delta - 1$ (or fewer) qudits if the location of the corrupted qudits is already known (e.g., they have been stolen).

It is helpful to regard (5.12) as embodying two conditions: the obvious off-diagonal condition saying that the matrix elements of Q must vanish when $r \neq q$; and the diagonal condition which, since $f(Q)$ is an arbitrary complex-valued function of the operator Q, is nothing but the requirement that all diagonal elements of Q (inside the coding space) be identical. The off-diagonal condition has a clear analog in classical codes, whereas the diagonal one does not. Both must hold for all operators of size up to and including $\delta - 1$, but need not be satisfied for larger operators.

In the coding literature it is customary to distinguish *nondegenerate* codes for which $f(Q) = 0$ for all operators of size between 1 and $\delta - 1$, i.e., for *all* q and r

$$\langle \mathbf{c}_q | \, Q | \mathbf{c}_r \rangle = 0 \ \text{ for } \ 1 \le \mathrm{size}(Q) < \delta, \tag{5.13}$$

and *degenerate* codes for which $f(Q) \neq 0$ for at least one Q in the same range of sizes. See p. 444 of [NC00] for the motivation behind this somewhat peculiar terminology when δ is odd. In this chapter our focus is on nondegenerate codes. For the most part they seem to perform as well as degenerate codes, though there are examples of degenerate codes that provide a larger K for given values of n, δ, and D than all known nondegenerate codes. Examples are the $((6,2,3))_2$ [2] and $((25,2,9))_2$ codes mentioned in [CRSS98].

5.3.2 Graph codes

When each basis vector $|\mathbf{c}_q\rangle$ is a member of the graph basis, of the form (5.10) for some graph G, we shall say that the corresponding code is a *graph codes* associated with this graph. As noted in Sec. 5.1, this differs from the definition employed in [SW01, Schb, Scha], but agrees with that in more recent $D = 2$ studies [YCO, CSSZ09], because we do not concern ourselves with the processes of encoding and decoding. In what follows we shall always assume $\delta \geq 2$, since $\delta = 1$ is trivial. As the left side of (5.12) is linear in Q, it suffices to check it for appropriate operators drawn from the Pauli basis $\mathcal{Q}$ as defined in Sec. 5.2.1. It is helpful to note that for any $Q \in \mathcal{Q}$, any pair $|\mathbf{c}_q\rangle$ and $|\mathbf{c}_r\rangle$ of graph basis states and any n-tuple $\mathbf{a}$,

$$\begin{aligned} \langle \mathbf{c}_q \oplus \mathbf{a}| \, Q |\mathbf{c}_r \oplus \mathbf{a}\rangle &= \langle \mathbf{c}_q| \, Z^{-\mathbf{a}} Q Z^{\mathbf{a}} |\mathbf{c}_r\rangle \\ &= \omega^{\mu} \, \langle \mathbf{c}_q| \, Q |\mathbf{c}_r\rangle \end{aligned} \tag{5.14}$$

for some integer μ depending on Q and $\mathbf{a}$; see (5.10), (5.11) and (5.4). Therefore, if (5.12) is satisfied for some Q and a collection $\{|\mathbf{c}_q\rangle\}$ of codewords, the same will be true for the same Q and the collection $\{|\mathbf{c}_q \oplus \mathbf{a}\rangle\}$ (with an appropriate change in $f(Q)$). Thus we can, and hereafter always will, choose the first codeword to be

$$|\mathbf{c}_0\rangle = |0, 0, \ldots, 0\rangle = |G\rangle. \tag{5.15}$$

Analogous to Hamming distance in classical information theory we define the *Pauli distance* Δ between two graph basis states as

$$\Delta(\mathbf{c}_q, \mathbf{c}_r) = \Delta\left(|\mathbf{c}_q\rangle, |\mathbf{c}_r\rangle\right) := \min\{\text{size}(Q) : \langle \mathbf{c}_q| \, Q |\mathbf{c}_r\rangle \neq 0\}, \tag{5.16}$$

where it suffices to take the minimum for $Q \in \mathcal{Q}$, the Pauli basis. (Ket symbols can be omitted from the arguments of Δ when the meaning is clear.) Also note the identities

$$\begin{aligned} \Delta(\mathbf{c}_q, \mathbf{c}_r) &= \Delta(\mathbf{c}_r, \mathbf{c}_q) = \Delta(\mathbf{c}_q \oplus \mathbf{a}, \mathbf{c}_r \oplus \mathbf{a}) \\ &= \Delta(\mathbf{c}_0, \mathbf{c}_r \ominus \mathbf{c}_q), \end{aligned} \tag{5.17}$$

where $\mathbf{a}$ is any n-tuple, and $\ominus$ means difference mod D, see (5.11). The second equality is a consequence of (5.14). Note that if in (5.16) we minimize only over Q operations which are tensor products of Z's (no X's), Δ is exactly the Hamming distance between the n-tuples $\mathbf{c}_q$ and $\mathbf{c}_r$, see (5.10).

For the case $q = r$, where (5.16) gives 0 (for $Q = I$), we introduce a special *diagonal distance* Δ' which is the minimum size of the right side of (5.16) when one restricts Q to be an element of $\mathcal{Q}$ of size 1 or more. The diagonal distance does not depend on the particular value of $q = r$, but is determined solely by the graph state $|G\rangle$—see (5.14) with $r = q$—and thus by the graph G. This has the important consequence that if we consider a particular G and want to find the optimum

[2] While there seems to be no proof that the $((6,2,3))_2$ degenerate code has a larger K than any nondegenerate code with $n = 6$ and $\delta = 3$, some support comes from the fact that we performed an exhaustive search of all graphs with 6 vertices and did not find a nondegenerate graph code with $\delta = 3$ and $K > 1$. But the notion that this degenerate code is superior to nondegenerate codes is undercut by the observation that the well known nondegenerate $((5,2,3))_2$ code uses only 5 instead of 6 qubits to achieve equal values of K and δ.

codes for a given δ that is no larger than Δ', the collection of operators $Q \in \mathcal{Q}$ for which (5.12) needs to be checked will all have zero diagonal elements, $f(Q) = 0$, and we can use (5.13) instead of (5.12). In other words, for the graph in question and for $\delta \leq \Delta'$, all graph codes are nondegenerate, and in looking for an optimal code one need not consider the degenerate case. Our computer results in Sec. 5.4 are all limited to the range $\delta \leq \Delta'$ where no degenerate codes exist for the graph in question. Any code with $\delta > \Delta'$ will necessarily be degenerate, since there is at least one nontrivial Q for which (5.12) must be checked for the diagonal elements.

A code is *G-additive (graph-additive)* if given any two codewords $|\mathbf{c}_q\rangle$ and $|\mathbf{c}_r\rangle$ belonging to the code, $|\mathbf{c}_q \oplus \mathbf{c}_r\rangle$ is also a codeword. As shown in Sec. 5.5, this notion of additivity implies the code is additive in the sense of being a stabilizer code. For this reason, we shall omit the G in G-additive except in cases where it is essential to make the distinction. Codes that do not satisfy the additivity condition are called nonadditive. The additive property allows one to express all codewords as "linear combinations" of k suitably chosen codeword generators. This implies an additive code must have $K = D^r$, r an integer, whenever D is prime. We will see an example of this in Sec. 5.4 for $D = 2$.

The *quantum Singleton* (QS) bound [KL97]

$$n \geq \log_D K + 2(\delta - 1) \quad \text{or} \quad K \leq D^{n-2(\delta-1)} \tag{5.18}$$

is a simple but useful inequality. We shall refer to codes which saturate this bound (the inequality is an equality) as *quantum Singleton* (QS) codes. Some authors prefer the term MDS, but as it is not clear to us how the concept of "maximum distance separable," as explained in [MS77], carries over to quantum codes, we prefer to use QS.

5.3.3 Method

We are interested in finding "good" graph codes in the sense of a large K for a given n, δ, and D. The first task is to choose a graph G on n vertices, not a trivial matter since the number of possibilities increases rapidly with n. We know of no general principles for making this choice, though it is helpful to note, see App. 5.A, that the diagonal distance Δ' cannot exceed 1 plus the minimum over all vertices of the number of neighbors of a vertex. Graphs with a high degree of symmetry are, for obvious reasons, more amenable to analytic studies and computer searches than those with lower symmetry.

Given a graph G and a distance δ, one can in principle search for the best nondegenerate code by setting $|\mathbf{c}_0\rangle = |G\rangle$, finding a $|\mathbf{c}_1\rangle$ with $\Delta(\mathbf{c}_0, \mathbf{c}_1) \geq \delta$, after that $|\mathbf{c}_2\rangle$ with both $\Delta(\mathbf{c}_0, \mathbf{c}_2) \geq \delta$ and $\Delta(\mathbf{c}_1, \mathbf{c}_2) \geq \delta$, and so forth, until the process stops. However, this may happen before one finds the largest K, because a better choice could have been made for $|\mathbf{c}_q\rangle$ at some point in the process. Exhaustively checking all possibilities is rather time consuming, somewhat like solving an optimal packing problem.

In practice what we do is to first construct a lookup table containing the $D^n - 1$ Pauli distances from $|G\rangle$ to all of the other graph basis states, using an iterative process starting with all $Q \in \mathcal{Q}$ of size 1, then of size 2, etc. This process also yields the diagonal distance Δ'. As we are only considering nondegenerate codes, we choose some $\delta \leq \Delta'$, so that (5.13) can be used in place of (5.12), and use the table to identify the collection S of all graph basis states with a distance greater than or equal to δ from $|\mathbf{c}_0\rangle = |G\rangle$. If S is empty there are no other codewords, so $K = 1$. However, if S is not empty then K is at least 2, and a search for the optimum code (largest K) is carried out as follows.

We produce a graph $\mathcal{S}$ (not to be confused with G) in which the nodes are the elements of S, and an edge connects two nodes if the Pauli distance separating them—easily computed from the lookup table with the help of (5.17)—is *greater than or equal to* δ. An edge in this graph signifies that the nodes it joins are sufficiently (Pauli) separated to be candidates for the code, and an optimal code corresponds to a largest complete subgraph or *maximum clique* of $\mathcal{S}$. Once a maximum clique has

been found, the corresponding graph basis states, including $|\mathbf{c}_0\rangle$, satisfy (5.13) and span a coding space with the largest possible K for this graph G and this δ.

The maximum clique problem on a general graph is known to be NP-complete [GJ79] and hence computationally difficult, and we do not know if $\mathcal{S}$ has special properties which can be exploited to speed things up. We used the relatively simple algorithm described in [CP90] for finding a maximum clique, and this is the most time-consuming part of the search procedure.

The method just described finds additive as well as nonadditive codes. In fact one does not know beforehand whether the resultant code will be additive or not. If one is only interested in additive codes, certain steps can be modified to produce a substantial increase in speed as one only has to find a set of generators for the code.

5.4 Results

5.4.1 Introduction

Results obtained using methods described above are reported here for various sequences of graphs, each sequence containing graphs of increasing n while preserving certain basic properties. We used a computer search to find the maximum number K of codewords for each graph in the sequence, for distances $\delta \leq \Delta'$ and for $D = 2$ or 3, qubits and qutrits, up to the largest number n of qudits allowed by our resources (running time). Sometimes this revealed a pattern which could be further analyzed using analytic arguments or known bounds on the number of codewords.

In the case of distance $\delta = 2$ we can demonstrate the existence of QS codes for arbitrarily large values of n and D, except when n is odd and D is even, see Part A. In the later subsections we report a significant collection of $D = 2$ and 3 codes for $\delta = 2$, 3, and 4, including QS codes; codes which are the largest possible additive codes for that set of n, D and δ; and a new $((16, 128, 4))_2$ additive code.

Tables show the K found as a function of other parameters. The meaning of superscripts used in the tables is given below.

- a – Indicates the maximum clique search was terminated before completion. This means the code we found might not be optimal, i.e. there might be another code with larger K for this graph. We can only say the code is *maximal* in the sense that no codeword can be added without violating (5.13). Absence of this superscript implies no code with a larger K exists for this δ and this graph, either because the program did an exhaustive search, or because K saturates a rigorous bound.
- b – Indicates a nonadditive code. Codes without this superscript are additive.
- c – Indicates a QS code, one where K saturates the Singleton bound (5.18).
- d – Indicates this is not a QS code, but the largest possible *additive* (graph or other) code for the given n, δ and D, This follows from linear programming bounds in [Gra07] for $D = 2$ and [KKKS06] for $D = 3$, along with the fact, Sec. 5.3.2, that for an additive code, K must be an integer power of D when D is prime. A larger *nonadditive* code for this graph might still be possible in cases flagged with a as well as d.

5.4.2 Distance $\delta = 2$; bar and star graphs

It was shown in [CRSS98] that for $D = 2$ one can construct $\delta = 2$ QS codes for any even n, and similar codes for larger D are mentioned, without giving details, in [Rai99]. One way to construct graph codes with $\delta = 2$ is to use the method indicated in the proof, App. 5.B, of the following result.
Partition theorem. *Suppose that for a given D the vertices of a graph G on n qudits can be partitioned into two nonempty sets V_1 and V_2 with the property that for each vertex in V_1 the sum of*

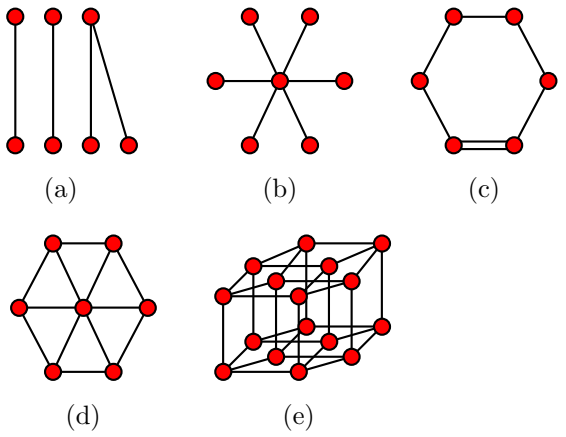

Figure 5.2: Examples from different graph sequences: (a) bar (odd n), (b) star, (c) cycle, (d) wheel, (e) $n = 16$ hypercube.

the number of edges (the sum of the multiplicities if multiple edges are present) joining it to vertices in V_2 is nonzero and coprime to D, and the same for the number of edges joining a vertex in V_2 to vertices in V_1. Then there is an additive QS code on G with distance $\delta = 2$.

A *bar* graph is constructed by taking n vertices and dividing them into two collections V_1 and V_2, of equal size when n is even, and one more vertex in V_2 when n is odd, as in Fig. 5.2(a). Next pair the vertices by connecting each vertex in V_1 by a single edge to a vertex in V_2, with one additional edge when n is odd, as shown in the figure. (Multiple edges are possible for $D > 2$, but provide no advantage in constructing codes.) When n is even the conditions of the partition theorem are satisfied: 1 is always coprime to D. For odd n, the last vertex in V_1 has 2 edges joining it to V_2, which is coprime to D when D is odd. Hence bar graphs yield $\delta = 2$ QS codes for all n when D is odd, and for even n when D is even.

A *star* graph, Fig. 5.2(b), has a *central* vertex joined by single edges to every *peripheral* vertex, and no edges connecting pairs of peripheral vertices. Since the diagonal distance Δ' is 2, nondegenerate star codes cannot have δ larger than 2. As in the case of bar codes, one can construct additive QS codes for any n when D is odd, and for even n when D is even [3] . For odd n and $D = 2$ there are nonadditive codes with

$$K(n) = 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}; \tag{5.19}$$

see App. 5.C for details. Codes with these parameters were discovered earlier by Smolin et al. [SSW07] using a different approach. Computer searches show that for all odd $n \leq 7$ star graphs cannot yield a K larger than (5.19).

5.4.3 Cycle graphs

We used computer searches to look for graph codes based on cycle (loop) graphs, Fig. 5.2(c). Table 5.1 shows the maximum number K of codewords for codes of distance $\delta = 2$ and $\delta = 3$ for both $D = 2$ qubits and $D = 3$ qutrits. In the qutrit case the best codes were obtained by including one double edge (weight 2), as in Fig. 5.2(c), though when n is odd equally good codes emerge with only single edges. In the qubit case all edges have weight 1.

[3] We omit the details. In some but not all cases one can use the Partition theorem with V_1 and V_2 the center and the peripheral vertices. Allowing some double edges when $D > 2$ extends the range of n values where the Partition theorem can be employed.

Table 5.1: Maximum K for qubit and qutrit cycle graphs. See Sec. 5.4.1 for detailed meaning of superscripts.

	$D=2$		$D=3$	
n	$\delta=2$	$\delta=3$	$\delta=2$	$\delta=3$
4	4^{c}	0	9^{c}	1^{c}
5	6^{b}	2^{c}	27^{c}	3^{c}
6	16^{c}	1	81^{c}	9^{c}
7	22^{b}	2^{d}	243^{c}	27^{c}
8	64^{c}	8^{d}	729^{c}	81^{c}
9	96^{ab}	12^{b}	2187^{c}	243^{c}
10	256^{c}	18^{b}	6561^{c}	729^{c}
11	272^{ab}	32^{ad}	19683^{c}	729^{ad}
12	1024^{c}	64^{ad}	59049^{c}	2187^{ad}

a Non-exhaustive search

b Nonadditive code

c Code saturating Singleton bound (5.18)

d Largest possible additive code

The $D=2$ entries in Table 5.1 include for $n=5$ the well known $((5,2,3))_2$, the nonadditive $((5,6,2))_2$ presented in [RHSS97], and, for larger n, a $((9,12,3))_2$ code similar to that in [YCLO08] and the $((10,18,3))_2$ of [CSSZ09] based upon the same graph.

The $D=3$, $\delta=3$ entries are interesting because the QS bound is saturated for $4 \le n \le 10$ but *not* for $n=11$. The $((11, 3^6 = 729, 3))_3$ code we found, the best possible *additive* code according to the linear programming bound in [KKKS06], falls short by a factor of 3 of saturating the $K = 3^7 = 2187$ QS bound, and even a nonadditive code based on this graph must have $K \le 1990$ [4] .

One can ask to what extent the results for $\delta=2$ in Table 5.1 could have been obtained, or might be extended to larger n, by applying the Partition theorem of Part A to a suitable partition of the cycle graph. It turns out—we omit the details—that when D is odd one can use the Partition theorem to produce codes that saturate the QS bound for any n, but when D is even the same approach only works when n is a multiple of 4. In particular, the $((6,16,2))_2$ additive QS code in Table 5.1 cannot be obtained in this fashion since the cycle graph cannot be partitioned in the required way.

5.4.4 Wheel graphs

If additional edges are added to a star graph so as to connect the peripheral vertices in a cycle, as in Fig. 5.2(d), the result is what we call a *wheel* graph. Because each vertex has at least three neighbors, our search procedure, limited to $\delta \le \Delta'$, can yield $\delta=4$ codes on wheel graphs, unlike cycle or star graphs. The construction of $\delta=2$ codes for any D is exactly the same as for star graphs, so in Table 5.2 we only show results for $\delta=3$ and 4, for both $D=2$ and 3. The $((16,128,4))_2$ additive code appears to be new, and its counterpart in the hypercube sequence is discussed below.

[4] Since the distance $\delta=3$ does not exceed the diagonal distance $\Delta'=3$ for this graph, a graph code is necessarily nondegenerate, see Sec. 5.3.2, and hence the quantum Hamming bound—see p. 444 of [NC00]—extended to $D=3$ applies, and this yields an upper bound of $K \le 1990$.

Table 5.2: Maximum K for qubit and qutrit wheel graphs. See Sec. 5.4.1 for detailed meaning of superscripts.

	$D=2$		$D=3$	
n	$\delta=3$	$\delta=4$	$\delta=3$	$\delta=4$
6	1	1^{c}	1	1^{c}
7	2^{d}	0	27^{c}	1
8	8^{d}	1^{d}	27	9^{c}
9	8^{d}	1^{d}	243^{c}	9
10	20^{c}	4^{d}	243^{a}	27
11	32^{ad}	4^{d}	729^{ad}	81
12	64^{ad}	8	2187^{ad}	81^{a}
13	128^{ad}	16	6561^{ad}	243^{a}
14	256^{ad}	32^{a}	19683^{ad}	729^{a}
15	512^{ad}	64^{ad}	59049^{ad}	2187^{a}
16	1024^{ad}	128^{ad}		

a Non-exhaustive search

b Nonadditive code

c Code saturating Singleton bound (5.18)

d Largest possible additive code

5.4.5 Hypercube graphs

Hypercube graphs, Fig. 5.2(e), have a high symmetry, and as n increases the coordination bound, App. 5.A, allows Δ' to increase with n, unlike the other sequences of graphs discussed above. We have only studied the $D = 2$ case, with the results shown in Table 5.3. Those for $\delta = 2$ are an immediate consequence of the Partition theorem: each hypercube is obtained by adding edges between two hypercubes of the next lower dimension, and these are the V_1 and V_2 of the theorem. The generators for the $((16, 128, 4))_2$ additive code are given in Table 5.4. The $2^7 = 128$ codewords are of the form, see (5.11), $|\alpha_1\mathbf{g}_1 \oplus \alpha_2\mathbf{g}_2 \oplus \cdots \alpha_7\mathbf{g}_7\rangle$, where each α_j can be either 0 or 1.

Table 5.3: Maximum K for qubit hypercube graphs. See Sec. 5.4.1 for detailed meaning of superscripts.

	$D=2$		
n	$\delta=2$	$\delta=3$	$\delta=4$
4	4^{c}	0	0
8	64^{c}	8^{d}	1^{d}
16	16384^{c}	512^{a}	128^{ad}

a Non-exhaustive search

c Code saturating Singleton bound (5.18)

d Largest possible additive code

Table 5.4: Generators of $((16, 128, 4))_2$ additive code for hypercube graph

Generator	Bit notation
$\|\mathbf{g}_1\rangle$	$\|0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1\rangle$
$\|\mathbf{g}_2\rangle$	$\|0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1\rangle$
$\|\mathbf{g}_3\rangle$	$\|0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,1\rangle$
$\|\mathbf{g}_4\rangle$	$\|0,0,0,0,0,0,0,1,1,0,1,0,0,0,1,0,0\rangle$
$\|\mathbf{g}_5\rangle$	$\|0,0,0,0,0,1,1,0,0,0,0,0,1,0,0,0,1\rangle$
$\|\mathbf{g}_6\rangle$	$\|0,0,1,1,0,0,0,0,0,1,0,0,0,1,0,0\rangle$
$\|\mathbf{g}_7\rangle$	$\|1,1,0,0,0,0,0,0,0,0,0,1,0,0,0,1\rangle$

5.5 G-Additive codes as stabilizer codes

The stabilizer formalism introduced by Gottesman in [Gotb] for $D = 2$ (qubits) provides a compact and powerful way of generating quantum error correcting codes. It has been extended to cases where D is prime or a prime power in [AK01, BB, KKKS06]. In [Schb] stabilizer codes were extended in a very general fashion to arbitrary D from a point of view that includes encoding. However, our approach to graph codes is somewhat different, see Sec. 5.1, and hence its connection with stabilizers deserves a separate discussion. We will show that for any $D \geq 2$ a G-additive (as defined near the end of Sec. 5.3.2) code is a stabilizer code, and the stabilizer is effectively a dual representation of the code.

The Pauli group $\mathcal{P}$ for general n and D was defined in Sec. 5.2.1. Relative to this group we define a *stabilizer* code (not necessarily a graph code) $\mathcal{C}$ to be a $K \geq 1$-dimensional subspace of the Hilbert space satisfying three conditions:

C1. There is a subgroup $\mathcal{S}$ of $\mathcal{P}$ such that for *every* T in $\mathcal{S}$ and *every* $|\psi\rangle$ in $\mathcal{C}$

$$T|\psi\rangle = |\psi\rangle \tag{5.20}$$

C2. The subgroup $\mathcal{S}$ is maximal in the sense that every T in $\mathcal{P}$ for which (5.20) is satisfied for all $|\psi\rangle \in \mathcal{C}$ belongs to $\mathcal{S}$.

C3. The coding space $\mathcal{C}$ is maximal in the sense that any ket $|\psi\rangle$ that satisfies (5.20) for every $T \in \mathcal{S}$ lies in $\mathcal{C}$.

If these conditions are fulfilled we call $\mathcal{S}$ the *stabilizer* of the code $\mathcal{C}$. That it is Abelian follows from (5.4), since for $K > 0$ there is some nonzero $|\psi\rangle$ satisfying (5.20). One can also replace (5.20) with

$$T|c_q\rangle = |c_q\rangle \tag{5.21}$$

where the $\{|c_q\rangle\}$ form an orthonormal basis of $\mathcal{C}$. Note that one can always find a subgroup $\mathcal{S}$ of $\mathcal{P}$ satisfying C1 and C2 for any subspace $\mathcal{C}$ of the Hilbert space, but it might consist of nothing but the identity. Thus it is condition C3 that distinguishes stabilizer codes from nonadditive codes. A stabilizer code is uniquely determined by $\mathcal{S}$ as well as by $\mathcal{C}$, since $\mathcal{S}$ determines $\mathcal{C}$ through C3.

As we shall see, the stabilizers of G-additive graph codes can be described in a fairly simple way. Let us begin with one qudit, $n = 1$, where the trivial graph G has no edges, and the graph basis states are of the form $\{Z^c|+\rangle\}$ for c in some collection C of integers in the range $0 \leq c \leq D-1$. The subgroup $\mathcal{S}$ of $\mathcal{P}$ satisfying C1 and C2 must be of the form $\{X^s\}$ for certain values of s, $0 \leq s \leq D-1$, belonging to a collection S. This is because Z and its powers map any state $Z^c|+\rangle$ to an orthogonal state, and hence T in (5.21) cannot possibly contain a (nontrivial) power of Z. Furthermore, since

$$X^s Z^c|+\rangle = \omega^{cs} Z^c|+\rangle, \tag{5.22}$$

see (5.2), X^s will leave $\{Z^c|+\rangle\}$ unchanged only if $\omega^{cs} = 1$, or

$$cs \equiv 0 \pmod{D}. \tag{5.23}$$

Thus for $\mathcal{S}$ to satisfy C1, it is necessary and sufficient that (5.23) hold for every $c \in C$, as well as every $s \in S$. Further, $\mathcal{S} = \{X^s\}$ is maximal in the sense of C2 only if S contains every s satisfying (5.23) for each $c \in C$. As shown in App. 5.D, such a collection S must either (depending on C) consist of $s = 0$ alone, or consist of the integer multiples νs_1, with $\nu = 0, 1, \ldots (D/s_1 - 1)$, of some $s_1 > 0$ that divides D. In either case, S is a subgroup of the group $\mathbb{Z}_D$ of integers under addition mod D, and indeed any such subgroup must have the form just described.

We now take up C3. Given the maximal collection S of solutions to (5.23), we can in turn ask for the collection of C' of integers c in the range 0 to $D-1$ that satisfy (5.23) for every s in S. Obviously, C' contains C, but as shown in App. 5.D, $C' = C$ if and only if C is a subgroup of $\mathbb{Z}_D$, i.e., $\mathcal{C}$ is G-additive. Next note that every T in $\mathcal{S}$, as it is a power of X and because of (5.22), maps every graph basis state to itself, up to a phase. Thus when (and only when) $\mathcal{C}$ is G-additive, the codewords are just those graph basis states for which this phase is 1 for every $T \in \mathcal{S}$. To check C3, expand an arbitrary $|\psi\rangle$ in the graph basis. Then $T|\psi\rangle = |\psi\rangle$ for all $T \in \mathcal{S}$ means that all coefficients must vanish for graph basis states that do not belong to $\mathcal{C}$. Hence C3 is satisfied if and only if $\mathcal{C}$ is G-additive.

The preceding analysis generalizes immediately to $n > 1$ in the case of the trivial graph G^0 with no edges. A graph code $\mathcal{C}$ has a basis of the form $\{Z^{\mathbf{c}}|G^0\rangle\}$ for a collection C of integer n-tuples $\mathbf{c} \in \mathbb{Z}_D^n$, and is G-additive when the collection $C = \{\mathbf{c}\}$ is closed under component-wise addition mod D, i.e., is a subgroup of $\mathbb{Z}_D^n$. Whether or not $\mathcal{C}$ is G-additive, the subgroup $\mathcal{S}$ of $\mathcal{P}$ satisfying C1 and C2 consists of all operators of the form $X^{\mathbf{s}} = X_1^{s_1} X_2^{s_2} \cdots$ with the n-tuple $\mathbf{s}$ satisfying

$$\mathbf{c} \cdot \mathbf{s} := \sum_{l=1}^{n} c_l s_l \equiv \mathbf{0} \pmod{D} \tag{5.24}$$

for every $\mathbf{c} \in C$. Just as for $n = 1$, $\mathcal{S}$ cannot contain Pauli products with (nontrivial) powers of Z operators. Let S denote the collection of all such $\mathbf{s}$. The linearity of (5.24) means S is an additive subgroup of $\mathbb{Z}_D^n$.

One can also regard (5.24) as a set of conditions, one for every $\mathbf{s} \in S$, that are satisfied by certain $\mathbf{c} \in \mathbb{Z}_D^n$. The set C' of all these solutions is itself an additive subgroup of $\mathbb{Z}_D^n$, and contains C. In App. 5.D we show that $C' = C$ if and only if C (the collection we began with) is an additive subgroup of $\mathbb{Z}_D^n$, and when this is the case the sizes of C and S are related by

$$|C| \cdot |S| = D^n. \tag{5.25}$$

Just as for $n = 1$, any $X^{\mathbf{s}}$ maps a graph basis state for the trivial graph G^0—they are all product states—onto itself up to a multiplicative phase, and the same argument used above for $n = 1$ shows that C3 is satisfied for all $T \in \mathcal{S}$ if and only if $\mathcal{C}$ is G-additive.

To apply these results to a general graph G on n qubits, note that the unitary $\mathcal{U}$ defined in (5.7) provides, through (5.6) and (5.10), a one-to-one map of the graph basis states of the trivial G^0 onto the graph basis states of G. At the same time the one-to-one map $\mathcal{U}P\mathcal{U}^\dagger$ carries the $\mathcal{S}$ satisfying C1 and C2 (and possibly C3) for the G^0 code to the corresponding $\mathcal{S}$, satisfying the same conditions for the G code. (The reverse maps are obtained by interchanging $\mathcal{U}^\dagger$ and $\mathcal{U}$.) Consequently, the results obtained for G^0 apply at once to G, and the transformation allows the elements of the stabilizer for the G graph code to be characterized by integer n-tuples $\mathbf{s}$ satisfying (5.24). Thus we have shown that G-additive codes are stabilizer codes, and for these the coding space and stabilizer group descriptions are dual, related by (5.24): each can be derived from the other.

5.6 Conclusion and discussion

In this chapter we have developed an approach to graph codes which works for qudits with general dimension D, and employs graphical methods to search for specific examples of such codes. It is similar to the approaches developed independently in [CSSZ09, YCO, HTZ+08]. We have used it for computer searches on graphs with a relatively small number n of qudits, and also to construct certain families of graphs yielding optimum distance $\delta = 2$ codes for various values of D and n which can be arbitrarily large. It remains a challenging problem to do the same for codes with distance $\delta > 2$.

In a number of cases we have been able to construct what we call quantum Singleton (QS) codes that saturate the quantum Singleton bound [KL97]: these include the $\delta = 2$ codes for arbitrarily large n and D mentioned above, and also a number of $\delta = 3$ codes in the case of $D = 3$ (qutrits), see Tables 5.1 and 5.2. The results for cycle graphs for $D = 3$ and $\delta = 3$ in Table 5.1 are interesting in that the QS bound is saturated for $n \leq 10$, but fails for $n = 11$, as it must for nondegenerate codes; see the discussion in Sec. 5.4.3. Our results are consistent with the difficulty of finding QS codes for larger δ [Gra07], but suggest that increasing D may help, as observed in [SW01]. It is worth noting that we have managed to construct many of the previously known nonadditive codes, or at least codes with the same $((n, K, \delta))_D$, using simple graphs. Some other nonadditive codes not discussed here, such as the $((10, 24, 3))_2$ code in [YCO], can also be obtained from suitably chosen graphs. While all these results are encouraging, they represent only a beginning in terms of understanding what properties of graphs lead to good graph codes, and how one might efficiently construct such codes with arbitrarily large n and δ, for various D.

As noted in Sec. 5.3.2, all graph codes with distance $\delta \leq \Delta'$, where Δ' is the diagonal distance of the graph, are necessarily nondegenerate, and our methods developed for such codes will (in principle) find them all. All codes with $\delta > \Delta'$ are necessarily degenerate codes, and their systematic study awaits further work. It should be noted that our extension of graph codes to $D > 2$ is based on extending Pauli operators in the manner indicated in [HDM05]. Though the extension seems fairly natural, and it is hard to think of alternatives when D is prime, there are other ways to approach the matter when D is composite (including prime powers), which could yield larger or at least different codes, so this is a matter worth exploring.

The relationship between stabilizer (or additive) codes and G-additive (as defined in Sec. 5.3.2) graph codes has been clarified by showing that they are dual representations, connected through a simple equation, (5.24), of the same thing. One might suspect that such duality extends to nongraphical stabilizer codes, but we have not studied the problem outside the context of graph codes. Nonadditive codes, which—if one uses our definition, Sec. 5.5—do not have stabilizers, are sometimes of larger size than additive codes, so they certainly need to be taken into account in the search for optimal codes. The graph formalism employed here works in either case, but computer searches are much faster for additive codes.

5.A The X-Z rule and related

X-Z Rule. *Acting with an X operator on the i'th qudit of a graph state $|G\rangle$ produces the same graph basis state as the action of Z operators on the neighbors of qudit i, raised to the power given by the edge multiplicities Γ_{im}.*

The operator X_i commutes with C_{lm} when $i \neq l$ and $i \neq m$, but if $i = l$ (or similarly $i = m$) one can show using (5.5) and (5.1) that

$$X_l C_{lm} = C_{lm} Z_m X_l = Z_m C_{lm} X_l. \tag{5.26}$$

That is, an X_i operator can be pushed from left to right through a C_{lm} with at most the cost of producing a Z operator associated with the *other* qudit: if $i = l$ one gets Z_m, if $i = m$ one gets Z_l.

Since all Z commute with all C, one can place the resulting Z_m either to the left or to the right of C_{lm}.

Now consider pushing X_i from the left to the right through $\mathcal{U}$, the product of C_{lm} operators defined in (5.7). Using (5.26) successively for those C_{lm} that do not commute with X_i, one sees that this can be done at the cost of generating a Z_m for every edge of the graph connecting i to another vertex m. Let the product of these be denoted as $\hat{Z} := \prod_{(l=i,m)\in E} Z_m^{\Gamma_{lm}}$. Then, with definition (5.6), we can show

$$\begin{aligned} X_i|G\rangle = X_i\mathcal{U}|G^0\rangle &= \hat{Z}\mathcal{U}X_i|G^0\rangle \\ &= \hat{Z}\mathcal{U}|G^0\rangle = \hat{Z}|G\rangle, \end{aligned} \tag{5.27}$$

which completes the proof of the X-Z Rule.

For graph codes satisfying (5.13), the X-Z Rule leads to the:

Coordination bound. *The diagonal distance Δ' for a graph G cannot exceed $\nu+1$, where ν is the minimum over all vertices of the number of neighbors of a vertex, this being the number of vertices joined to the one in question by edges, possibly of multiplicity greater than 1.*

To make the counting absolutely clear consider Fig. 5.1, where the vertex on the left has 3 neighbors, and each of the others has 1 neighbor, so that in this case $\nu = 1$. To derive the bound, apply X to a vertex which has ν neighbors. By the X-Z rule the result is the same as applying appropriate powers of Z to each neighbor. Let P be this X tensored with appropriate compensating powers of Z at the neighboring vertices in such a way that $P|G\rangle = |G\rangle$. The size of P is $\nu+1$, and Δ' can be no larger.

Another useful result follows from the method of proof of the X-Z Rule:

Paulis to Paulis. *Let P be a Pauli product* (5.3)*, and for $\mathcal{U}$ defined in* (5.7) *let*

$$P' = \mathcal{U}^\dagger P \mathcal{U}, \quad P'' = \mathcal{U} P \mathcal{U}^\dagger. \tag{5.28}$$

Then both P' and P'' are Pauli products.

To see why this works, rewrite the first equality as $\mathcal{U}P' = P\mathcal{U}$, and imagine pushing each of the single qudit operators, of the form $X_j^{\mu_j} Z_j^{\nu_j}$, making up the product P through $\mathcal{U}$ from left to right. This can always be done, see the discussion following (5.26), at the cost of producing some additional Z operators, which can be placed on the right side of $\mathcal{U}$, to make a contribution to P'. At the end of the pushing the final result can be rearranged in the order specified in (5.3) at the cost of some powers of ω, see (5.2). The argument for P'' uses pushing in the opposite direction.

5.B Partition theorem proof

Given the partition of the n qudits into sets V_1 and V_2 containing n_1 and n_2 elements, the code of interest consists of the graph basis states $|\mathbf{c}\rangle = |c_1, c_2, \ldots, c_n\rangle$ satisfying the two conditions

$$\sum_{i\in V_1} c_i \equiv 0 \pmod{D} \tag{5.29}$$

$$\sum_{j\in V_2} c_j \equiv 0 \pmod{D} \tag{5.30}$$

This code is additive and contains $K = D^{n_1-1} \times D^{n_2-1} = D^{n-2}$ codewords. (The counting can be done by noting that (5.29) defines a subgroup of the additive group $\mathbb{Z}_D^{n_1}$, and its cosets are obtained by replacing 0 with some other integer on the right side of (5.29).)

We first demonstrate that this code has $\delta \geq 2$ by showing that any Pauli operator, except the identity, applied to a single qudit maps a codeword into a graph basis state not in the code. If Z^ν for $0 < \nu < D$ is applied to a qudit in V_1, the effect will be to replace 0 on the right side of (5.29)

with ν, so this graph state is not in the code. If X^μ, $0 < \mu < D$ is applied to a qudit in V_1 the result according to the X-Z Rule, App. 5.A, will be the same as placing Z operators on neighboring qudits in V_2 (as well as V_1) in such a way that 0 on the right side of (5.30) is replaced by $g\mu$, where g is the total number of edges (including multiplicities) joining the V_1 qudit with qudits in V_2. But as long as g is coprime to D, as specified in the condition for the theorem, $g\mu$ cannot be a multiple of D, and (5.30) will no longer be satisfied. The same is true if $Z^\nu X^\mu$ is a applied to a qudit in V_1. Obviously the same arguments work for Pauli operators applied to a single qudit in V_2. Thus we have shown that $\delta \geq 2$.

But $\delta > 2$ is excluded by the QS bound, so we conclude that we have an additive code of $K = D^{n-2}$ elements and distance $\delta = 2$ that saturates the QS bound.

5.C Construction of qubit star graph codes

As noted in Sec. 5.4.2 a star graph for n-qubits consists of a central vertex joined by edges to $n-1$ peripheral vertices. Let V_1 be the central vertex and V_2 the set of peripheral vertices. When n is even and $D = 2$ the conditions of the Partition theorem, Sec. 5.4.2, are satisfied, and the $\delta = 2$ code constructed in App. 5.B consists of the 2^{n-2} graph basis states with no Z on the central qubit and an even number r of Z's on the peripheral qubits, thus satisfying (5.29) and (5.30), and yielding an additive QS code.

When n is odd the central vertex is connected to an even number $n-1$ of vertices in V_2, so the conditions of the Partition theorem no longer hold. A reasonably large $\delta = 2$ nonadditive code can, however, be constructed by again assuming no codeword has Z on the central qubit, and that the code contains all graph basis states with r Z's on the peripheral qubits *for a certain selected set R of r values*.

The set R must satisfy two conditions. First, it cannot contain both r and $r+1$, because applying an additional Z to a codeword with r Z's yields one with $r+1$, and one cannot have both of them in a code of distance $\delta = 2$. Second, applying X to the central vertex and using the X-Z rule, App. 5.A, maps a codeword with r Z's to one with $r' = n-1-r$; hence R cannot contain both r and $n-1-r$. For example, when $n = 7$ ($n-1 = 6$ peripheral qubits) the set $R = \{0, 2, 5\}$ satisfies both conditions, as does $R = \{1, 4, 6\}$, whereas $R = \{1, 2, 6\}$ violates the first condition and $R = \{1, 3, 5\}$ the second.

By considering examples of this sort, and noting that the number of such graph basis states with r Z's is $\binom{n-1}{r}$ which is equal to $\binom{n-1}{n-1-r}$, one sees that for n odd one can construct in this way a nonadditive code with

$$\sum_{i=0}^{(n-3)/2} \binom{n-1}{i} = 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2} \tag{5.31}$$

codewords.

5.D Solutions to $\mathbf{c} \cdot \mathbf{s} \equiv 0 \pmod{D}$

Let $\mathcal{A}$ be the collection of all n-component integer vectors (i.e., n-tuples) of the form $\mathbf{a} = (a_1, a_2, \ldots a_n)$, $0 \leq a_j \leq D-1$, with component-wise sums and scalar multiplication defined using arithmetic operations mod D. In particular, $\mathcal{A}$ is a group of order D^n under component-wise addition mod D. We shall be interested in subsets C and $\mathcal{S}$ of $\mathcal{A}$ that satisfy

$$\mathbf{c} \cdot \mathbf{s} := \sum_{l=1}^{n} c_l s_l \equiv 0 \pmod{D} \tag{5.32}$$

for all $\mathbf{c} \in C$ and $\mathbf{s} \in S$. Given some collection C, we shall say that S is *maximal* relative to C if it includes *all* solutions $\mathbf{s}$ that satisfy (5.32) for every $\mathbf{c} \in C$. It is easily checked that a maximal S

is an additive subgroup of $\mathcal{A}$: it includes the zero vector and $-\mathbf{s}$ mod D whenever $\mathbf{s} \in S$. A similar definition holds for C being maximal relative to a given S. We use $|C|$ to denote the number of elements in a set or collection C.

Theorem. *Let C be an additive subgroup of $\mathcal{A}$, and let S be maximal relative to C, i.e., the set of all $\boldsymbol{s}$ that satisfy* (5.32) *for every $\boldsymbol{c} \in C$. Then C is also maximal relative to S, and*

$$|C| \cdot |S| = D^n. \tag{5.33}$$

The proof is straightforward when D is a prime, since $\mathbb{Z}_D$ is a field, and one has the usual rules for a linear space. The composite case is more difficult, and it is useful to start with $n = 1$:

Lemma. Let C be a subgroup under addition mod D of the integers lying between 0 and $D-1$, and S all integers in the same range satisfying

$$cs \equiv 0 \pmod{D} \tag{5.34}$$

for every $c \in C$. Then C consists of *all* integers c in the range of interest which satisfy (5.34), and $|C| \cdot |S| = D$.

When $C = \{0\}$ the proof is obvious, since $|C| = 1$ and $|S| = D$. Otherwise, because it is an additive subgroup of $\mathbb{Z}_D$, C consists of the multiples $\{\mu c_1\}$ of the smallest positive integer c_1 in C, necessarily a divisor of D, when μ takes the values $0, 1, \ldots s_1 - 1$, where $s_1 = D/c_1$. One quickly checks that all integer multiples $s = \nu s_1$ of this s_1 satisfy (5.34) and are thus contained in S. But S is also an additive subgroup, and s_1 is its minimal positive element (except in the trivial case $c_1 = 1$), for were there some smaller positive integer s' in S we would have $0 < c_1 s' < D$, contradicting (5.34). Similarly there is no way to add any additional integers to C while preserving the subgroup structure under addition mod D without including a positive c less than c_1, which will not satisfy (5.34) for $s = s_1$.

For $n > 1$ it is helpful to use a *generator matrix* F, with components F_{rl}, each between 0 and $D-1$, with the property that $\mathbf{c} \in C$ if and only if it can be expressed as linear combinations of rows of F, i.e.,

$$c_l \equiv \sum_r b_r F_{rl} \pmod{D} \tag{5.35}$$

for a suitable collection of integers $\{b_r\}$. This collection will of course depend on the $\mathbf{c}$ in question, and for a given $\mathbf{c}$ need not be unique, even assuming (as we shall) that $0 \le b_r \le D-1$. In particular the matrix F for which each row is a distinct $\mathbf{c}$ in C, with r running from 1 to $|C|$, is a generator matrix. It is straightforward to show that if F is any generator matrix for C, S consists of all solutions $\mathbf{s}$ to the equations

$$\sum_{l=1}^{n} F_{rl} s_l \equiv 0 \pmod{d} \text{ for } r = 1, 2, \ldots. \tag{5.36}$$

The collections C and S, vectors of the form (5.35) and those satisfying (5.36), remain the same if F is replaced by another generator matrix F' obtained by one of the following *row operations*: (i) permuting two rows; (ii) multiplying (mod D) any row by an *invertible* integer, i.e., an integer which has a multiplicative inverse mod D; (iii) adding (mod D) to one row an *arbitrary* multiple (mod D) of a different row; (iv) discarding (or adding) any row that is all zeros, to get a matrix of a different size. Of these, (i) and (iv) are obvious, and (ii) is straightforward. For (iii), consider what happens if the second row of F is added to the first, so that $F'_{rl} = F_{rl}$ except for

$$F'_{1l} \equiv F_{1l} + F_{2l} \pmod{D}. \tag{5.37}$$

Then setting

$$b'_1 = b_1,\ b'_2 \equiv b_2 - b_1 \pmod{d},\ b'_l = b_l \text{ for } l \ge 3 \tag{5.38}$$

leads to the same $\mathbf{c}$ in (5.35) if b and F are replaced by b' and F' on the right side. Likewise, any $\mathbf{c}$ that can be written as a linear combination of F' rows can be written as a combination of those of F, so the two matrices generate the same collection C, and hence have the same solution set S to (5.36). Since adding to one row a different row can be repeated an arbitrary number of times, (iii) holds for an arbitrary (not simply an invertible) multiple of a row.

The corresponding column operations on a generator matrix are (i) permuting two columns; (ii) multiplying a column by an invertible integer; (iii) adding (mod D) to one column an arbitrary multiple (mod D) of a different column. Throwing away (or adding) columns of zeros is *not* an allowed operation. When column operations are carried out to produce a new F' from F, the new collections C' and S' obtained using (5.35) and (5.36) will in general be different, but C' is an additive subgroup of the same size (order), $|C'| = |C|$, and likewise $|S'| = |S|$. The argument is straightforward for (i) and (ii), and for (iii) it is an easy exercise to show that if the second column of F is added to the first to produce F', the collection C is mapped into C' by the map

$$c'_1 \equiv c_1 + c_2 \pmod{D}\,; \quad c'_l = c_l \text{ for } l \geq 2 \tag{5.39}$$

whose inverse will map C' into C when one generates F from F' by subtracting the second column from the first. Thus $|C| = |C'|$. The same strategy shows that $|S'| = |S|$; instead of (5.39) use $s'_2 \equiv s_2 - s_1 \pmod{D}$, and $s'_l = s_l$ for $l \neq 2$.

The row and column operations can be used to transform the generator matrix to a (non unique) diagonal form, in the following fashion. If each F_{rl} is zero the problem is trivial. Otherwise use row and column permutations so that the smallest positive integer f in the matrix is in the upper left corner $r = 1 = l$. Suppose f does not divide some element, say F_{13}, in the first row. Then by subtracting a suitable multiple of the first column from the third column we obtain a new generator F' with $0 < F'_{13} < f$, and interchanging the first and third columns we have a generator with a smaller, but still positive, element in the upper left corner. Continue in this fashion, considering both the first row and the first column, until the upper left element of the transformed generator divides *every* element in both. When this is the case, subtracting multiples of the first column from the other columns, and multiples of the first row from the other rows, will yield a matrix with all zeros in the first row and first column, apart from the nonzero upper left element at $r = 1 = l$, completing the first step of diagonalization.

Next apply the same overall strategy to the sub matrix obtained by ignoring the first row and column. Continuing the process of diagonalization and discarding rows that are all zero (or perhaps adding them back in again), one arrives at a diagonal $n \times n$ generator matrix

$$\hat{F}_{rl} = f_l \delta_{rl}, \tag{5.40}$$

where some of the f_l may be zero. The counting problem is now much simplified, because for each l c_l can be any multiple mod D of f_l, and s_l any solution to $f_l s_l \equiv 0 \pmod{D}$, independent of what happens for a different l. Denoting these two collections by C_l and S_l, the lemma implies that $|C_l| \cdot |S_l| = D$ for every l, and taking the product over l from 1 to n yields (5.33). This in turn implies that C consists of *all possible* $\mathbf{c}$ that satisfy (5.32) for all the $\mathbf{s} \in S$. To see this, note that the size $|C|$ of C is $D^n/|S|$. If we interchange the roles of C and S in the above argument (using a generator matrix for S, etc.), we again come to the result (5.33), this time interpreting $|C|$ as the number of solutions to (5.32) with S given. Thus since it cannot be made any larger, the original additive subgroup C we started with is maximal relative to S. This completes the proof.

6

Location of quantum information in additive graph codes

6.1 Introduction

Quantum codes in which quantum information is redundantly encoded in a collection of code carriers play an important role in quantum information, in particular in systems for error correction and in schemes for quantum communication [Sch95, Sho95, BBP$^+$96, CS96]. They are a generalization of the classical codes well known and widely used in everyday communication systems [MS77]. While for the latter it is fairly obvious where the information is located, the quantum case is more complicated for two reasons. First, a quantum Hilbert space with its non-commuting operators is a more complex mathematical structure than the strings of bits or other integers used in classical codes. Second, the very concept of "information" is not easy to define in the quantum case. However, in certain cases one is able to make quite precise statements. Thus in the five qubit code [LMPZ96] that encodes one qubit of information, none of the encoded information is present in any two qubits taken by themselves, whereas all the information can be recovered from any set of three qubits [Gri05].

Similar precise statements can be made, as we shall see, in the case of an *additive graph code* on a collection of n qudits which constitute the *carriers* of the code, provided each qudit has the same dimension D, with D some integer greater than one (not necessarily prime). It was shown in [LYGG08] that all additive graph codes are stabilizer codes, and in [Schb, GKR] that all stabilizer codes are equivalent to graph codes for prime D. A detailed discussion of non-binary quantum error correcting codes can be found in [Gota, Rai99, SW01, HTZ$^+$08, LYGG08]. The five qubit code just mentioned is an example of a quantum code that is locally equivalent to an additive graph code [SW01], and the information location has an "all or nothing" character. In general the situation is more interesting in that some subset of carriers may contain some but not all of the encoded information, and what is present can be either "classical" or "quantum," or a mixture of the two. Since many of the best codes currently known are additive graph codes, identifying the location of information could prove useful when utilizing codes for error correction, or designing new or better codes, or codes that correct some types of errors more efficiently than others [IM07]. Our formalism can also be applied to study quantum secret sharing schemes employing graph states and can even handle a more general setting where there might be subsets that contain partial information and hence are neither authorized (contain the whole quantum secret) nor unauthorized (contain no information whatsoever about the secret).

Our approach to the problem of information location is algebraic, based upon the fact that generalized Pauli operators on the Hilbert space of the carriers form a group. Subgroups of this group can be associated with different types of information, and the information available in some

subset of the carriers can also be identified with, or is isomorphic to, an appropriate subgroup, as indicated in the isomorphism theorem of Sec. 6.5. In the process of deriving this theorem we go through a series of steps which amount to an *encoding procedure* that takes the initial quantum information and places it in the coding subspace of the carrier Hilbert space. These steps can in turn be transformed into a set of quantum gates to produce an explicit circuit that carries out the encoding. This result, although somewhat subsidiary to our main aims, is itself not without interest, and is an alternative to a previous scheme [SW01] limited to prime D.

There have been some previous studies of quantum channels using an algebraic approach similar to that employed here. Those most closely related to our work are by Bény et al. [BKK07a, BKK07b] (and see Bény [Bén]) and Blume-Kohout et al. [BKNPV08]. These authors have provided a set of very general conditions under which an algebraic structure is preserved by a channel. In App. 6.D we show that our results fit within the framework of a "correctable algebra" as defined in [BKK07a, BKK07b, Bén]. See also the remarks in Sec. 6.7.

The remainder of this chapter is organized as follows. Some general comments about types of quantum information and their connection with certain ideal quantum channels are found in Sec. 6.2. Section 6.3 contains definitions of the Pauli group and of some quantum gates used later in the chapter. The formalism associated with additive graph codes as well as our encoding strategy is in Sec. 6.4; this along with some results on partial traces leads to the fundamental isomorphism result in Sec. 6.5, which also indicates some of its consequences for the types of information discussed in Sec. 6.2. Section 6.6 contains various applications to specific codes, for both qubit and qudit carriers. Finally, Sec. 6.7 contains a summary, conclusions, and some open questions. Appendices 6.A and 6.B contain longer proofs of theorems, App. 6.C presents an efficient linear algebra based algorithm for working out the results for any additive graph code, and App. 6.D illustrates the connection with related work in [BKK07a] and [BKK07b].

6.2 Types of information

Both classical and quantum information theory have to do with statistical correlations between properties of two or more systems, or properties of a single system at two or more times. In the classical case information is always related to a possible set of physical properties that are distinct and mutually exclusive—e.g., the voltage has one of a certain number of values—with one and only one of these properties realized in a particular system at a particular time. For quantum systems it is useful to distinguish different *types* or *species* of information [Gri07], each corresponding to a collection of mutually distinct properties represented by a (projective) decomposition $\mathcal{J} = \{J_j\}$ of the identity I on the relevant Hilbert space $\mathcal{H}$:

$$I = \sum_j J_j, \quad J_j = J_j^\dagger = J_j^2, \quad J_j J_k = \delta_{jk} J_j. \tag{6.1}$$

Any normal operator M has a spectral representation of the form

$$M = \sum_j \mu_j J_j, \tag{6.2}$$

where the μ_j are its eigenvalues, and the decomposition $\{J_j\}$ is uniquely specified by requiring $\mu_j \neq \mu_k$ when $j \neq k$. This means one can sensibly speak about the type of information $\mathcal{J}(M)$ *associated with* a normal operator M. When M is Hermitian this is the kind of information obtained by measuring M.

This terminology allows one to discuss the transmission of information through a quantum channel in the following way. Let $\mathcal{E}$ be the completely positive, trace preserving superoperator that maps the space of operators $\mathcal{L}(\mathcal{H})$ of the channel input onto the corresponding operator space $\mathcal{L}(\mathcal{H}')$ of

the channel output $\mathcal{H}'$ (which may have a different dimension from $\mathcal{H}$). Provided

$$\mathcal{E}(J_j)\mathcal{E}(J_k) = 0 \text{ for } j \neq k, \tag{6.3}$$

for all the operators $\{J_j\}$ associated with a decomposition $\mathcal{J}$ of the $\mathcal{H}$ identity, we shall say the channel is *ideal* or *noiseless* for the $\mathcal{J}$ species of information, or, equivalently, the $\mathcal{J}$ type of information is *perfectly present* in the channel output $\mathcal{H}'$. Formally, each physical property J_j at the input corresponds in a one-to-one fashion to a unique property, the support of $\mathcal{E}(J_j)$ (or the corresponding projector) at the output. Thus we have a quantum version of a noiseless classical channel, a device for transmitting symbols, in this case the label j on J_j, from the input to the output by associating distinct symbols with distinct physical properties—possibly a different collection of properties at the output than at the input.

The opposite extreme from a noiseless channel is one in which $\mathcal{E}(J_j)$ is *independent of* j up to a multiplicative constant. In this case no information of type $\mathcal{J}$ is available at the channel output: the channel is *blocked*, or completely noisy; equivalently, the $\mathcal{J}$ species of information is *absent* from the channel output. Hereafter we shall always use "absent" in the strong sense of "completely absent", and the term *present*, or *partially present* for situations in which some type of information is not (completely) absent but is also not perfectly present: i.e., the channel is noisy but not completely blocked for this type of information.

In some cases all the projectors in $\{J_j\}$ will be of rank 1, onto pure states, but in other cases some or all of them may be of higher rank, in which case one may have a *refinement* $\mathcal{L} = \{L_l\}$ of $\{J_j\}$ such that each projector J_j is a sum of one or more projectors from the $\mathcal{L}$ decomposition. It is then clear that if the $\mathcal{L}$ information is absent/perfectly present from/in the channel output the same is true of the $\mathcal{J}$ information, but the converse need not hold. Thus it may be that the coarse grained $\mathcal{J}$ information is perfectly present, but no additional information is available about the refinement. A particularly simple situation, which we will encounter later, is one in which the output $\mathcal{H}'$ is itself a tensor product, say $\mathcal{H}'_1 \otimes \mathcal{H}'_2$, $\mathcal{J}$ a decomposition of $\mathcal{H}'_1$, $\mathcal{J} = \{J_j \otimes I\}$ and $\mathcal{K}$ a decomposition of $\mathcal{H}'_2$, $\mathcal{K} = \{I \otimes K_k\}$. It can then be the case that the information associated with the $\mathcal{J}$ decomposition is perfectly present and that associated with the $\mathcal{K}$ decomposition is (perfectly) absent from the channel output.

Suppose $\mathcal{J} = \{J_j\}$ and $\mathcal{K} = \{K_k\}$ are two types of quantum information defined on the same Hilbert space. The species $\mathcal{J}$ and $\mathcal{K}$ are *compatible* if all the projectors in $\mathcal{J}$ commute with all the projectors in $\mathcal{K}$, in which case the distinct nonzero projectors in the collection $\{J_j K_k\}$ provide a common refinement of the type discussed above. Otherwise, if some projectors in one collection do not commute with certain projectors in the other, $\mathcal{J}$ and $\mathcal{K}$ are *incompatible* and cannot be combined with each other. This is an example of the single framework rule of consistent quantum reasoning, [Gri96] or Ch. 16 of [Gri02]. The same channel may be ideal for some $\mathcal{J}$ and blocked for some $\mathcal{K}$, or noisy for both but with different amounts of noise. From a quantum perspective, classical information theory is only concerned with a single type of (quantum) information, or several compatible types which possess a common refinement, whereas the task of quantum, in contrast to classical, information theory is to analyze situations where multiple incompatible types need to be considered.

The term "classical information" when used in a quantum context can be ambiguous or misleading. Generally it is used when only a single type of information, corresponding to a single decomposition of the identity, suffices to describe what emerges from a channel, and other incompatible types can therefore be ignored. Even in such cases it is helpful to indicate explicitly which decomposition of the identity is involved if that is not obvious from the context. The contrasting term "quantum information" can then refer to situations where two or more types of information corresponding to incompatible decompositions are involved, and again it is helpful to be explicit about what one has in mind if there is any danger of ambiguity.

An *ideal quantum channel* is one in which there is an isometry V from $\mathcal{H}$ to $\mathcal{H}'$ such that

$$\mathcal{E}(A) = VAV^\dagger \tag{6.4}$$

for every operator A on $\mathcal{H}$. In this case the superoperator $\mathcal{E}$ preserves not only sums but also operator products:

$$\mathcal{E}(AB) = \mathcal{E}(A)\mathcal{E}(B). \tag{6.5}$$

Conversely, if (6.5) holds for any pair of operators, one can show that the quantum channel is ideal [BKK07a, BKK07b], i.e. $\mathcal{E}$ has the form (6.4). As the isometry maps orthogonal projectors to orthogonal projectors, (6.3) will be satisfied for every species of information, and we shall say that *all* information is perfectly present at the channel output. The converse, that a channel which is ideal for all species, or even for an appropriately chosen pair of incompatible species is an ideal quantum channel, is also correct; see [Gri05, Gri07].

The preservation of operator products, (6.5), can be a very useful tool in checking for the presence or absence of various types of information in the channel output, as we shall see in Sec. 6.5. When (6.5) holds for arbitrary A and B belonging to a particular decomposition of the identity, this suffices to show that the channel is ideal for this species. However, note that this sufficient condition is not necessary, since (6.3) could hold without the $\mathcal{E}(A_j)$ being projectors, in which case $\mathcal{E}(A_j^2)$ is not mapped to $\mathcal{E}(A_j)^2$.

We use the term *ideal classical channel* for a type of information $\mathcal{J} = \{J_j\}$ to refer to a situation where (6.3) is satisfied and, in addition,

$$\mathcal{E}(J_j A J_k) = 0 \text{ for } j \neq k, \tag{6.6}$$

where A is any operator on the input Hilbert space $\mathcal{H}$. That is, not only is type $\mathcal{J}$ perfectly transmitted, but all other types are "truncated" relative to this type, in the notation of [Gri96].

6.3 Preliminary remarks and definitions

6.3.1 Generalized Pauli operators on n qudits

We generalize Pauli operators to higher dimensional systems of arbitrary dimension D in the following way. The X and Z operators acting on a single qudit are defined as

$$Z = \sum_{j=0}^{D-1} \omega^j |j\rangle\langle j|, \quad X = \sum_{j=0}^{D-1} |j\rangle\langle j+1|, \tag{6.7}$$

and satisfy

$$X^D = Z^D = I, \quad XZ = \omega ZX, \quad \omega = \mathrm{e}^{2\pi \mathrm{i}/D}, \tag{6.8}$$

where *the addition of integers is modulo D*, as will be assumed from now on. For a collection of n qudits we use subscripts to identify the corresponding Pauli operators: thus Z_i and X_i operate on the space of qudit i. The Hilbert space of a single qudit is denoted by $\mathcal{H}$, and the Hilbert space of n qudits by $\mathcal{H}_n$, respectively. Operators of the form

$$\omega^\lambda X^{\mathbf{x}} Z^{\mathbf{z}} := \omega^\lambda X_1^{x_1} Z_1^{z_1} \otimes X_2^{x_2} Z_2^{z_2} \otimes \cdots \otimes X_n^{x_n} Z_n^{z_n} \tag{6.9}$$

will be referred to as *Pauli products*, where λ is an integer in $\mathbb{Z}_D$ and $\mathbf{x}$ and $\mathbf{z}$ are n-tuples in $\mathbb{Z}_D^n$, the additive group of n-tuple integers mod D. For a fixed n the collection of all possible Pauli products (6.9) form a group under operator multiplication, the *Pauli group* $\mathcal{P}_n$. If p is a Pauli product, then $p^D = I$ is the identity operator on $\mathcal{H}_n$, and hence the order of any element of $\mathcal{P}_n$ is either D or else an integer that divides D. While $\mathcal{P}_n$ is not abelian, it has the property that two elements *commute up to a phase*: $p_1 p_2 = \omega^{\lambda_{12}} p_2 p_1$, with λ_{12} an integer in $\mathbb{Z}_D$ that depends on p_1 and p_2.

The collection of Pauli products with $\lambda = 0$, i.e. a pre-factor of 1, is denoted by $\mathcal{Q}_n$ and forms an orthonormal basis of $\mathcal{L}(\mathcal{H}_n)$, the Hilbert space of linear operators on $\mathcal{H}_n$, with respect to the inner product

$$\frac{1}{D^n} \mathrm{Tr}[q_1^\dagger q_2] = \delta_{q_1,q_2}, \quad \forall q_1, q_2 \in \mathcal{Q}_n. \tag{6.10}$$

Note that $\mathcal{Q}_n$ is a *projective group* or group up to phases. There is a bijective map between $\mathcal{Q}_n$ and the quotient group $\mathcal{P}_n/\{\omega^\lambda I\}$ for $\lambda \in \mathbb{Z}_D$ where $\{\omega^\lambda I\}$, the center of $\mathcal{P}_n$, consists of phases multiplying the identity operator on n qudits.

6.3.2 Generalization of qubit quantum gates to higher dimensions

In this subsection we define some one and two qudit gates generalizing various qubit gates. The qudit generalization of the Hadamard gate is the *Fourier gate*

$$\mathrm{F} := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} \omega^{jk} |j\rangle \langle k| \,. \tag{6.11}$$

For an invertible integer $q \in \mathbb{Z}_D$ (i.e. integer for which there exists $\bar{q} \in \mathbb{Z}_D$ such that $q\bar{q} \equiv 1 \bmod D$), we define a *multiplicative gate*

$$\mathrm{S}_q := \sum_{j=0}^{D-1} |j\rangle \langle jq| \,, \tag{6.12}$$

where qj means multiplication mod D. The requirement that q be invertible ensures that S_q is unitary; for a qubit S_q is just the identity.

For two distinct qudits a and b we define the CNOT gate as

$$\mathrm{CNOT}_{ab} := \sum_{j=0}^{D-1} |j\rangle \langle j|_a \otimes X_b^j = \sum_{j,k=0}^{D-1} |j\rangle \langle j|_a \otimes |k\rangle \langle k+j|_b \,, \tag{6.13}$$

the obvious generalization of the qubit Controlled-NOT, where a labels the control qudit and b labels the target qudit. Next the SWAP gate is defined as

$$\mathrm{SWAP}_{ab} := \sum_{j,k=0}^{D-1} |k\rangle \langle j|_a \otimes |j\rangle \langle k|_b \,. \tag{6.14}$$

It is easy to check that SWAP gate is hermitian and does indeed swap qudits a and b. Unlike the qubit case, the qudit SWAP gate is not a product of three CNOT gates, but can be expressed in terms of CNOT gates and Fourier gates as

$$\mathrm{SWAP}_{ab} = \mathrm{CNOT}_{ab}(\mathrm{CNOT}_{ba})^\dagger \mathrm{CNOT}_{ab}(\mathrm{F}_a^2 \otimes I_b), \tag{6.15}$$

with

$$(\mathrm{CNOT}_{ba})^\dagger = (\mathrm{CNOT}_{ba})^{D-1} = (I_a \otimes \mathrm{F}_b^2)\mathrm{CNOT}_{ba}(I_a \otimes \mathrm{F}_b^2). \tag{6.16}$$

Finally we define the generalized Controlled-phase or CP gate as

$$\mathrm{CP}_{ab} = \sum_{j=0}^{D-1} |j\rangle \langle j|_a \otimes Z_b^j = \sum_{j,k=0}^{D-1} \omega^{jk} |j\rangle \langle j|_a \otimes |k\rangle \langle k|_b \,. \tag{6.17}$$

The CP and CNOT gates are related by a local Fourier gate, similar to the qubit case

$$\mathrm{CNOT}_{ab} = (I_a \otimes \mathrm{F}_b)\mathrm{CP}_{ab}(I_a \otimes \mathrm{F}_b)^\dagger, \tag{6.18}$$

since F maps Z into X under conjugation (see Table 6.1).

The gates F, S_q, SWAP, CNOT and CP are unitary operators that map Pauli operators to Pauli operators under conjugation, as can be seen from Tables 6.1 and 6.2. They are elements of the so called *Clifford group* on n qudits [Gota, HDM05], the group of n-qudit unitary operators that leaves $\mathcal{P}_n$ invariant under conjugation, i.e. if O is a Clifford operator, then $\forall p \in \mathcal{P}_n$, $OpO^\dagger \in \mathcal{P}_n$. From Tables 6.1 and 6.2 one can easily deduce the result of conjugation by F, S_q, SWAP, CNOT and CP on *any* Pauli product.

Pauli operator	S_q	F
Z	Z^q	X
X	$X^{\bar{q}}$	Z^{D-1}

Table 6.1: The conjugation of Pauli operators by one-qudit gates F and S_q ($\bar{q}$ is the multiplicative inverse of q mod D).

Pauli product	CNOT_{ab}	SWAP_{ab}	CP_{ab}
$I_a \otimes Z_b$	$Z_a \otimes Z_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$
$Z_a \otimes I_b$	$Z_a \otimes I_b$	$I_a \otimes Z_b$	$Z_a \otimes I_b$
$I_a \otimes X_b$	$I_a \otimes X_b$	$X_a \otimes I_b$	$Z_a^{D-1} \otimes X_b$
$X_a \otimes I_b$	$X_a \otimes X_b^{D-1}$	$I_a \otimes X_b$	$X_a \otimes Z_b^{D-1}$

Table 6.2: The conjugation of Pauli products on qudits a and b by two-qudit gates CNOT, SWAP and CP. For the CNOT gate, the first qudit a is the control and the second qudit b the target.

6.4 Graph states, graph codes and related operator groups

6.4.1 Graph states and graph codes

Let $G = (V, E)$ be a graph with n vertices V, each corresponding to a qudit, and a collection E of undirected edges connecting pairs of distinct vertices (no self loops). Two qudits can be joined by multiple edges, as long as the multiplicity does not exceed $D-1$. The graph G is completely specified by the *adjacency matrix* Γ, where the matrix element Γ_{ab} represents the number of edges that connect vertex a with vertex b. The *graph state*

$$|G\rangle = U|G_0\rangle = U\left(|+\rangle^{\otimes n}\right) \tag{6.19}$$

is obtained by applying the unitary (Clifford) operator

$$U = \prod_{(a,b)\in E} \left(\mathrm{CP}_{ab}\right)^{\Gamma_{ab}}, \tag{6.20}$$

where each pair (a, b) of vertices occurs only once in the product, to the *trivial graph state*

$$|G_0\rangle := |+\rangle^{\otimes n}, \tag{6.21}$$

with

$$|+\rangle := \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |j\rangle. \tag{6.22}$$

Define $\mathcal{S}^G$ to be the stabilizer of $|G\rangle$, the subgroup of operators from $\mathcal{P}_n$ that leave $|G\rangle$ unchanged. The stabilizer $\mathcal{S}_0^G$ of the trivial graph state $|G_0\rangle$ is simply the set of all X-type Pauli products with no additional phases,

$$\mathcal{S}_0^G = \left\{X^{\mathbf{x}} : \mathbf{x} = (x_1, x_2, \ldots, x_n)\right\}, \tag{6.23}$$

where x_j are arbitrary integers between 0 and $D-1$. Since $|G\rangle$ is related to $|G_0\rangle$ through a Clifford operator (see (6.19) and (6.20)), it follows at once that the stabilizer $\mathcal{S}^G$ of $|G\rangle$ is related to the stabilizer $\mathcal{S}_0^G$ of the trivial graph through the Clifford conjugation

$$\mathcal{S}^G = U\mathcal{S}_0^G U^\dagger, \tag{6.24}$$

with U defined in (6.20).

A *graph code* C can be defined as the K-dimensional subspace $\mathcal{H}_C$ of $\mathcal{H}_n$ spanned by a collection of K mutually orthogonal codewords

$$|\mathbf{c}_j\rangle = Z^{\mathbf{c}_j}|G\rangle, \quad j = 1, 2, \ldots, K \tag{6.25}$$

where

$$\mathbf{c}_j = (c_{j1}, c_{j2}, \ldots, c_{jn}) \tag{6.26}$$

is for each j an n-tuple in $\mathbb{Z}_D^n$. The c_{jk} notation suggests a matrix $\mathbf{c}$ with K rows and n columns, of integers between 0 and $D-1$, and this is a very helpful perspective. In this chapter we are concerned with *additive* graph codes, meaning that the rows of this matrix form a group under component-wise addition mod D, isomorphic to the abelian *coding group* $\mathcal{C}$, of order $|\mathcal{C}| = K$, of the operators $Z^{\mathbf{c}_j}$ under multiplication. We use $(\mathcal{C}, |G\rangle)$ to denote the corresponding graph code. For more details about graph states and graph codes for arbitrary D, see [LYGG08].

Note that the codeword $(0, 0, \ldots, 0)$ is just the graph state $|G\rangle$, and in the case of the trivial graph $|G_0\rangle$ this is the tensor product of $|+\rangle$ states, (6.21), not the tensor product of $|0\rangle$ states which the n-tuple notation $(0, 0, \ldots, 0)$ might suggest. Overlooking this difference can lead to confusion through interchanging the role of X and Z operators, which is the reason for pointing it out here.

6.4.2 The encoding problem

A coding group $\mathcal{C}$ can be used to create an additive code starting with any n qudit graph state, including the trivial graph $|G_0\rangle$, because the entangling unitary U commutes with $Z^{\mathbf{z}}$ for any $\mathbf{z}$; thus

$$|\mathbf{c}_j\rangle = Z^{\mathbf{c}_j}U|G_0\rangle = UZ^{\mathbf{c}_j}|G_0\rangle = U|\mathbf{c}_j^0\rangle \tag{6.27}$$

where the $|\mathbf{c}_j^0\rangle$ span the code $(\mathcal{C}, |G_0\rangle)$. But in addition the coding group $\mathcal{C}$ is isomorphic, as explained below to a *trivial* code $\mathcal{C}_0$,

$$\mathcal{C}_0 = \langle Z_1^{m_1}, Z_2^{m_2}, \ldots, Z_k^{m_k}\rangle \tag{6.28}$$

which is *generated by*, i.e., includes all products of, the operators inside the angular brackets $\langle\ \rangle$. Here k is an integer less than or equal to n, and each m_j is 1 or a larger integer that divides D. The simplest situation is the one in which each of the m_j is equal to 1, in which case $\mathcal{C}_0$ is nothing but the group, of order D^k, of products of Z operators to any power less than D on the first k qudits. One can think of these qudits as comprising the input system through which information enters the code, while the remaining $n-k$ qudits, each initially in a $|+\rangle$ state, form the ancillary system for the encoding operation.

If, however, one of the m_j is greater than 1, the corresponding generator $Z_j^{m_j}$ is of order

$$d_j = D/m_j, \tag{6.29}$$

and represents a qudit of dimensionality d_j rather than D. Thus for example, if $D = 6$ and $m_1 = 2$, applying Z_1^2 and its powers to $|+\rangle$ will produce three orthogonal states corresponding to a qutrit, $d_1 = 3$. (Identifying operators Z and X on these three states which satisfy (6.8) with $D = 3$ is not altogether trivial, and is worked out in Sec. 6.4.3 below.) In general one can think of the group $\mathcal{C}_0$ in (6.28) as associated with a collection of k qudits, the j'th qudit having dimension d_j, and therefore the collection as a whole a dimension of $K = d_1 d_2 \cdots d_k$, equal to that of the graph code. If one thinks of the information to be encoded as initially present in these k qudits, the encoding problem is how to map them in an appropriate way into the coding subspace $\mathcal{H}$ of the n (D-dimensional) carriers.

We address this by first considering the connection between $\mathcal{C}$ and $\mathcal{C}_0$ in a simple example with $n = 3$, $D = 6$, and

$$\mathcal{C} = \left\langle Z_1^4 Z_2^3 Z_3^3, Z_2^3 Z_3^3 \right\rangle, \tag{6.30}$$

a coding group of order 6. The two generators in (6.30) correspond, in the notation introduced in (6.26), to the rows of the 2×3 matrix

$$\mathbf{f} = \begin{pmatrix} 4 & 3 & 3 \\ 0 & 3 & 3 \end{pmatrix}. \tag{6.31}$$

By adding rows or multiplying them by constants mod D one can create 4 additional rows which together with those in (6.31) constitute the 6×3 $\mathbf{c}$ matrix.

Through a sequence of elementary operations mod D—a) interchanging of rows/columns, b) multiplication of a row/column by an *invertible* integer, c) addition of any multiple of a row/column to a *different* row/column—a matrix such as $\mathbf{f}$ can be converted to the Smith normal form [New72, Sto96]

$$\mathbf{s} = \mathbf{v} \cdot \mathbf{f} \cdot \mathbf{w}, \tag{6.32}$$

where $\mathbf{v}$ and $\mathbf{w}$ are invertible (in the mod D sense) square matrices, and $\mathbf{s}$ is a diagonal rectangular matrix, as in (6.33). It is proved in [Sto96] that a $K \times n$ matrix can be reduced to the Smith form in only $\mathcal{O}(K^{\theta-1}n)$ operations from $\mathbb{Z}_D$, where θ is the exponent for matrix multiplication over the ring $\mathbb{Z}_D$, i.e. two $m \times m$ matrices over $\mathbb{Z}_D$ can be multiplied in $\mathcal{O}(m^\theta)$ operations from $\mathbb{Z}_D$. Using standard matrix multiplication $\theta = 3$, but better algorithms [CW87] allow for $\theta = 2.38$.

For the example above, the sequence

$$\begin{pmatrix} 4 & 3 & 3 \\ 0 & 3 & 3 \end{pmatrix} \to \begin{pmatrix} 4 & 0 & 0 \\ 0 & 3 & 3 \end{pmatrix} \to \begin{pmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = \mathbf{s} \tag{6.33}$$

proceeds by adding the second row of $\mathbf{f}$ to the first (mod 6), then the second column to the third column, and finally multiplying the first row by 5 (which is invertible mod 6). The final step is needed so that the diagonal elements divide D: $m_1 = 2$, $m_2 = 3$, so that $d_1 = 3$ and $d_2 = 2$. Thus we arrive at the trivial coding group

$$\mathcal{C}_0 = \left\langle Z_1^2, Z_2^3 \right\rangle, \tag{6.34}$$

isomorphic to $\mathcal{C}$ in (6.30).

Since the procedure for reducing a matrix to Smith normal form is quite general, the procedure illustrated in this example can be applied to any coding group $\mathcal{C}$, as defined following (6.26), to find a corresponding trivial coding group $\mathcal{C}_0$. The row operations change the collection of generators but not the coding group that they generate; i.e., the final collection of K rows is the same. The column operations, on the other hand, produce a different, but isomorphic, coding group, and one can think of these as realized by a unitary operator W which is a product of various SWAP, CNOT and S_q gates, so that

$$\mathcal{C} = W\mathcal{C}_0W^\dagger, \tag{6.35}$$

that is, conjugation by W maps each operator in $\mathcal{C}_0$ to its counterpart in $\mathcal{C}$. In our example, $W = \mathrm{CNOT}_{32}$ is the only column operation, the second arrow in (6.33), and represents the first step in the encoding circuit for this example, Fig. 6.1(b). It is left as an exercise to check that this relates the generators in (6.30) and (6.34) through (6.35). Table 6.3 indicates how different matrix column operations are related to the corresponding gates in the encoding circuit.

The overall encoding operation

$$|\mathbf{c}_j\rangle = UW|\mathbf{c}_j^0\rangle \tag{6.36}$$

starting with the trivial code on the trivial graph $(\mathcal{C}_0, |G_0\rangle)$ and ending with the desired code $(\mathcal{C}, |G\rangle)$ is shown for our example in Fig. 6.1(b) for the case of a graph indicated in (a) in this figure. It is important to notice that both W and U, and therefore their product, are Clifford operators, unitaries that under conjugacy map Pauli products to Pauli products. This follows from the fact that the gates in Table 6.3 are Clifford gates, and will allow us in what follows to extend arguments that are relatively straightforward for trivial codes on trivial graphs to more general additive graph codes.

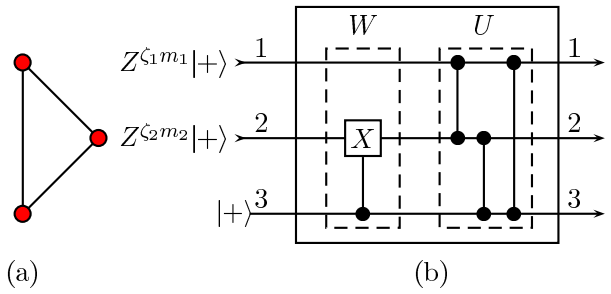

Figure 6.1: (a) The graph state used in the example; (b) The encoding circuit: the input states $Z_1^{\zeta_1 m_1} Z_2^{\zeta_2 m_2} |++\rangle$ that correspond to the trivial code $\mathcal{C}_0$ are mapped by W to $\mathcal{C}$, then U entangles the qudits. Here $m_1 = 2$, $m_2 = 3$ and ζ_j are integers such that $0 \leqslant \zeta_j \leqslant d_j - 1$, with $d_1 = 3$, $d_2 = 2$.

Matrix operation in $\mathbb{Z}_D$	Clifford conjugation
Interchange of columns a and b	SWAP_{ab}
Multiplication of column a by invertible integer q	S_q on qudit a
Addition of m times column b to column a	$(\mathrm{CNOT}_{ab})^m$

Table 6.3: The correspondence between matrix column operations in $\mathbb{Z}_D$ and conjugation by Clifford gates. For the CNOT gate, the first qudit a is the control and the second qudit b the target.

6.4.3 The information group

In this section we define the *information group* that plays a central role in the isomorphism theorem in Sec. 6.5 below. The basic strategy is most easily understood in terms of $C_0 = (\mathcal{C}_0, |G_0\rangle)$, the trivial code on the trivial graph. However, because the overall encoding map UW in (6.36) is a Clifford operation mapping Pauli products to Pauli products, various results that apply to C_0 can be immediately translated to the general graph code $C = (\mathcal{C}, |G\rangle)$ we are interested in, and for this reason most of the formulas valid for both are written in the form valid for C even if the derivations are based on C_0.

The pointwise stabilizer[1] of C_0, the subgroup of operators from $\mathcal{P}_n$ that leave every codeword $|\mathbf{c}_j^0\rangle$ unchanged, is given by

$$\mathcal{S}_0 = \left\{ X^{\mathbf{x}} : \mathbf{x} = (\eta_1 d_1, \eta_2 d_2, \ldots, \eta_k d_k, x_{k+1}, \ldots, x_n) \right\}, \tag{6.37}$$

where the d_j are defined in (6.29), η_j is any integer between 0 and $m_j - 1$, and the x_j for $j > k$ are arbitrary integers between 0 and $D - 1$. That this is correct can be seen as follows. First, Pauli products belonging to $\mathcal{S}_0$ cannot contain Z_j operators, for such operators map each codeword onto an orthogonal state. On the other hand, every $X_j^{x_j}$ leaves $|G_0\rangle$, (6.21), unchanged, so it belongs to $\mathcal{S}_0$ if and only if it commutes with $Z_j^{m_j}$, which means $x_j m_j$ must be a multiple of D, or x_j a multiple of d_j, see (6.29). Thus elements of $\mathcal{S}_0$ commute with elements of $\mathcal{C}_0$, (6.28). Since its operators cannot alter the phases of the codewords, no additional factors of ω^λ are allowed, and

[1] Also called the "fixer" or "fixator". It is important to distinguish this subgroup from the group theoretical notion of the stabilizer of the coding space in the sense of the subgroup of $\mathcal{P}_n$ that maps the coding space onto itself without necessarily leaving the individual vectors fixed. As we shall not employ the latter, it should cause no confusion if we hereafter follow the usual convention in quantum codes and omit "pointwise," even though retaining it would add some precision.

thus $\mathcal{S}_0$ is given by (6.37). The stabilizer of the (nontrivial) code C is then the isomorphic group $\mathcal{S}$ obtained using the unitary UW of (6.36):

$$\mathcal{S} = (UW)\mathcal{S}_0(UW)^\dagger \equiv \{(UW)s(UW)^\dagger \ : s \in \mathcal{S}_0\}, \tag{6.38}$$

a collection of Pauli products because the unitary UW, as remarked earlier, is a Clifford unitary. The order of $\mathcal{S}_0$, and thus of $\mathcal{S}$, is given by

$$|\mathcal{S}| = D^{n-k}\prod_{j=1}^{k} m_j = \frac{D^n}{\prod_{j=1}^{k} d_j} = \frac{D^n}{|\mathcal{C}|} = \frac{D^n}{K}. \tag{6.39}$$

Next define the subgroup $\mathcal{W}$ of $\mathcal{P}_n$

$$\mathcal{W} = \langle \mathcal{S}^G, \mathcal{C}\rangle \tag{6.40}$$

generated by operators belonging to the stabilizer $\mathcal{S}^G$ of the graph state or to the coding group $\mathcal{C}$, and denote it by $\mathcal{W}_0 = \langle \mathcal{S}_0^G, \mathcal{C}_0\rangle$ in the case of the trivial code. The elements of $\mathcal{S}_0$ commute with those of $\mathcal{S}_0^G$ (both are abelian and the former is a subgroup of the latter), and also with those of $\mathcal{C}_0$, as noted above. As group properties are preserved under the UW map, as in (6.38), we conclude that all elements in $\mathcal{S}$ commute with those in $\mathcal{W}$, even though $\mathcal{W}$ is not (in general) abelian, and hence $\mathcal{S}$ is a normal subgroup of $\mathcal{W}$. Now define the *abstract information group* as the quotient group

$$\overline{\mathcal{G}} = \mathcal{W}/\mathcal{S} = \langle \mathcal{S}^G, \mathcal{C}\rangle/\mathcal{S} \tag{6.41}$$

consisting of cosets of $\mathcal{S}$, written as $g\mathcal{S}$ or $\mathcal{S}g$ for g in $\mathcal{W}$. Note that because any element g of $\mathcal{W}$ is a Pauli product, $g^D = I$ is the identity, and the order of g is either D or an integer that divides D. Consequently the order of any element of $\overline{\mathcal{G}}$ is also D or an integer that divides D.

To understand the significance of $\overline{\mathcal{G}}$ consider a trivial code on a single qudit, with

$$\mathcal{C}_0 = \langle Z_1^{m_1}\rangle, \quad \mathcal{S}_0^G = \langle X_1\rangle, \quad \mathcal{S}_0 = \langle X_1^{d_1}\rangle \tag{6.42}$$

The elements of $\overline{\mathcal{G}}_0$ can be worked out using its identity $\bar{I}$ and the generators $\bar{X}$ and $\bar{Z}$:

$$\begin{aligned}
\bar{I} &= \mathcal{S}_0 = \{I_1, X_1^{d_1}, X_1^{2d_1}, \ldots\}\\
\bar{X} &= X_1\mathcal{S}_0 = \{X_1, X_1^{d_1+1}, X_1^{2d_1+1}, \ldots\}\\
\bar{Z} &= Z_1^{m_1}\mathcal{S}_0 = \{Z_1^{m_1}, Z_1^{m_1}X_1^{d_1}, \ldots\}.
\end{aligned} \tag{6.43}$$

It is evident that the cosets $\bar{X}$, $\bar{X}^2 = X_1^2\mathcal{S}_0$ and so forth up to $\bar{X}^{d_1-1}$ are distinct, whereas $\bar{X}^{d_1} = \bar{I} = \mathcal{S}_0$. The same is true for powers of $\bar{Z}$. Furthermore,

$$\bar{X}\bar{Z} = X_1Z_1^{m_1}\mathcal{S}_0 = \omega^{m_1}Z_1^{m_1}X_1\mathcal{S}_0 = \bar{\omega}\bar{Z}\bar{X}, \tag{6.44}$$

with $\bar{\omega} = \omega^{m_1} = \mathrm{e}^{2\pi\mathrm{i}/d_1}$. Thus $\overline{\mathcal{G}}_0$ is generated by operators $\bar{X}$ and $\bar{Z}$ that satisfy (6.8) with D replaced by d_1, which is to say the corresponding group is what one would expect for a qudit of dimension d_1. The same argument extends easily to the trivial code on k carriers produced by $\mathcal{C}_0$, see (6.28): $\overline{\mathcal{G}}_0$ is isomorphic to the group of Pauli products on a set of qudits of dimension $d_1, d_2, \ldots, d_k$. The same structure is inherited by the abstract information group $\overline{\mathcal{G}}$ for the code $C = (\mathcal{C}, |G\rangle)$ obtained by applying the UW map as in (6.38).

The abstract information group $\overline{\mathcal{G}}$ is isomorphic to the *information group* $\mathcal{G}$ of *information operators* acting on the coding space $\mathcal{H}_C$ and defined in the following way. Its identity is the operator

$$P = |\mathcal{S}|^{-1}\Sigma(\mathcal{S}) = |\mathcal{S}|^{-1}\sum_{s\in\mathcal{S}} s, \tag{6.45}$$

where $\Sigma(\mathcal{A})$ denotes the sum of the operators that make up a collection $\mathcal{A}$. In fact, P is just the projector onto $\mathcal{H}_C$, as can be seen as follows. Since $\mathcal{S}$ is a group, $P^2 = P$; and since a group contains the inverse of every element, and $s \in \mathcal{S}$ is unitary (a Pauli product), $P^\dagger = P$. These two conditions mean that P is a projector onto some subspace of $\mathcal{H}_n$. Since $\mathcal{S}$ is the (pointwise) stabilizer of the coding space each s in $\mathcal{S}$ maps a codeword onto itself, and thus P maps each codeword to itself. Consequently, all the codewords lie in the space onto which P projects. Finally, the rank of P is

$$\mathrm{Tr}[P] = D^n/|\mathcal{S}| = |\mathcal{C}| = K \tag{6.46}$$

(see (6.39)), since the trace of every s in $\mathcal{S}$ is zero except for the identity with trace D^n. (Note that while $\mathcal{P}_n$ contains the identity multiplied by various phases, only the identity operator occurs in $\mathcal{S}$.) Therefore P projects onto $\mathcal{H}_C$, and is given by the formula

$$P = \sum_{j=1}^{K} |\mathbf{c}_j\rangle\langle\mathbf{c}_j|. \tag{6.47}$$

The other information operators making up the information group $\mathcal{G} = \{\hat{g}\}$ are formed in a similar way from the different cosets making up $\mathcal{W}/\mathcal{S}$:

$$\hat{g} = |\mathcal{S}|^{-1}\Sigma(g\mathcal{S}) = gP = PgP = P\hat{g}P. \tag{6.48}$$

That is, for each coset form the corresponding sum of operators and divide by the order of the stabilizer $\mathcal{S}$. The second and third equalities in (6.48) reflect the fact that the product of the cosets $\mathcal{S}$ and $g\mathcal{S}$ in either order is $g\mathcal{S}$, which is to say P forms the group identity of $\mathcal{G}$. They also tell us that the operators that make up $\mathcal{G}$ act only on the coding space, mapping $\mathcal{H}_C$ onto itself, and give zero when applied to any element of $\mathcal{H}_n$ in the orthogonal complement of $\mathcal{H}_C$. Because $\mathcal{S}$ is a normal subgroup of $\mathcal{W}$, products of operators of the form (6.48) mirror the products of the corresponding cosets, so the map from the abstract $\overline{\mathcal{G}}$ to the group $\mathcal{G}$ is a homomorphism. That it is actually an isomorphism is a consequence of the following, proved in App. 6.A:

Lemma 6.1. *Let $\mathcal{R}$ be a linearly independent collection of Pauli product operators that form a subgroup of $\mathcal{P}_n$, and for a Pauli product p let $p\mathcal{R} = \{pr : r \in \mathcal{R}\}$. Then*

i) The operators in $p\mathcal{R}$ are linearly independent.

ii) If p and q are two Pauli products, one or the other of the following two mutually exclusive possibilities obtains:

α)

$$p\mathcal{R} = \mathrm{e}^{\mathrm{i}\phi} q\mathcal{R} \tag{6.49}$$

in the sense that each operator in $p\mathcal{R}$ is equal to $\mathrm{e}^{\mathrm{i}\phi}$ times an operator in $q\mathcal{R}$

β) The union $p\mathcal{R} \cup q\mathcal{R}$ is a collection of $2|\mathcal{R}|$ linearly independent operators.

Since the collection of Pauli products $\mathcal{Q}_n$ with fixed phase forms a basis of $\mathcal{L}(\mathcal{H}_n)$, a collection of Pauli products can be linearly *dependent* if and only if it contains both an operator and that operator multiplied by some phase. As the (pointwise) stabilizer $\mathcal{S}$ leaves each codeword unchanged, the corresponding operators are linearly independent, and the lemma tells us that distinct cosets $g\mathcal{S} \neq h\mathcal{S}$ give rise to distinct operators $\hat{g} \neq \hat{h}$. Either $g\mathcal{S} = \mathrm{e}^{\mathrm{i}\phi} h\mathcal{S}$, in which case $\hat{g} = \mathrm{e}^{\mathrm{i}\phi}\hat{h} \neq \hat{h}$ (since if $\mathrm{e}^{\mathrm{i}\phi} = 1$ the cosets are identical). Or else the $g\mathcal{S}$ operators are linearly independent of the $h\mathcal{S}$ operators, and therefore $\hat{g}$ and $\hat{h}$ are linearly independent. Consequently the homomorphic map from $\overline{\mathcal{G}}$ to $\mathcal{G}$ is a bijection, and the two groups are isomorphic.

The single qudit example considered in (6.42) provides an example of how $\overline{\mathcal{G}}$ and $\mathcal{G}$ are related. In this case the projector

$$P_0 = (1/m_1)(I_1 + X_1^{d_1} + \cdots) \tag{6.50}$$

projects onto the subspace spanned by $|+\rangle, Z_1^{m_1}|+\rangle, Z_1^{2m_1}|+\rangle, \ldots$. While each of the operators that make up a coset such as $\bar{X}$ in (6.43) is unitary, their sum, an operator times P_0, is no longer unitary, though when properly normalized acts as a unitary on the subspace onto which P_0 projects. That the different sums of operators making up the different cosets are distinct is in this case evident from inspection without the need to invoke Lemma 6.1.

Let us summarize the main results of this subsection. For an additive graph code C we have defined the information group $\mathcal{G}$ of operators acting on the coding subspace $\mathcal{H}_C$, whose group identity is the projector P onto $\mathcal{H}_C$. It is isomorphic to the group of Pauli products acting on a tensor product of qudits of dimensions d_1, d_2, ..., d_k, which can be thought of as the input to the code, see Sec. 6.4.2. Each element $\hat{g}$ of $\mathcal{G}$ is of the form $P\hat{g}P$, so as an operator on $\mathcal{H}_n$ it commutes with P and yields zero when applied to any vector in the orthogonal complement of $\mathcal{H}_C$. The dimension of $\mathcal{H}_C$ is $K = d_1 d_2 \cdots d_k$, the size of the code, and hence the elements of $\mathcal{G}$ span the space of linear operators $\mathcal{L}(\mathcal{H}_C)$ on $\mathcal{H}_C$.

6.5 Subsets of carriers and the isomorphism theorem

6.5.1 Subsets of carriers

Before stating the isomorphism theorem, which is the principal technical result of this chapter, let us review some facts established in Sec. 6.4. The additive graph code $(\mathcal{C}, |G\rangle)$ we are interested in can be thought of as arising from an encoding isometry that carries the channel input onto a subspace $\mathcal{H}_C$ of the n-qudit carrier space $\mathcal{H}_n$, as in Fig 6.1. This isometry, as explained in Sec. 6.2 in connection with (6.4), constitutes a perfect quantum channel, and thus all the information of interest can be said to be located in the $\mathcal{H}_C$ subspace, where it is represented by the information group $\mathcal{G}$, a multiplicative group of operators for which the projector P on $\mathcal{H}_C$ is the group identity, and which as a group is isomorphic to the abstract information group $\overline{\mathcal{G}}$ defined in (6.41).

We are interested in what kinds of information are available in some subset B of the carriers, where $\bar{B}$ denotes the complementary set. For this purpose it is natural to consider the partial traces over $\bar{B}$, i.e., the traces down to the Hilbert space $\mathcal{H}_B$, of the form

$$g_B = N^{-1}\mathrm{Tr}_{\bar{B}}[\hat{g}], \tag{6.51}$$

where $\hat{g}$ is an element of the information group $\mathcal{G}$, and the positive constant N is defined in (6.58) below. In those cases in which $g_B = 0$ the $\mathcal{J}(\hat{g})$ information has disappeared and is not available in the subset B, so we shall be interested in those $\hat{g}$ for which the partial trace does not vanish, that is to say in the elements of the *subset information group*

$$\mathcal{G}^B = \{\hat{g} \in \mathcal{G} : \mathrm{Tr}_{\bar{B}}[\hat{g}] \neq 0\}\,. \tag{6.52}$$

We show below that $\mathcal{G}^B$ is a subgroup of $\mathcal{G}$, thus justifying its name, and that it is isomorphic to the group $\mathcal{G}_B$ of nonzero operators of the form g_B defined in (6.51). To actually determine which elements of $\mathcal{G}$ belong to $\mathcal{G}^B$ one needs to take partial traces of the $\hat{g} \in \mathcal{G}$ to see which of them do not trace down to zero. In App. 6.C we present an efficient linear algebra algorithm based on solving systems of linear equations mod D that can find $\mathcal{G}^B$ in $\mathcal{O}(K^2 n^\theta)$ operations from $\mathbb{Z}_D$ where θ is defined in Sec. 6.4.2.

If an operator A on the full Hilbert space $\mathcal{H}_n$ of the n carriers can be written as a tensor product of an operator on $\mathcal{H}_B$ times the identity operator $I_{\bar{B}}$ on $\mathcal{H}_{\bar{B}}$ we shall say that A is *based in* B. Let $\mathcal{B}$ be the collection of all operators on $\mathcal{H}_n$ that are based in B. Obviously, $\mathcal{B}$ is closed under sums, products, and scalar multiplication. In addition the partial trace $\mathrm{Tr}_{\bar{B}}[A]$ of an operator A in $\mathcal{B}$ is "essentially the same" operator, apart from normalization in the sense that

$$A = D^{-|\bar{B}|} \cdot \mathrm{Tr}_{\bar{B}}[A] \otimes I_{\bar{B}}. \tag{6.53}$$

If $A \notin \mathcal{B}$ is a Pauli product, then its partial trace over $\bar{B}$ vanishes, since $\mathrm{Tr}[X]$ and $\mathrm{Tr}[Z]$ and their powers (when not equal to I) are zero. Consequently the partial trace over $\bar{B}$ of $\Sigma(g\mathcal{S})$ in (6.48) is the same as the partial trace of $\Sigma[(g\mathcal{S})\cap\mathcal{B}]$, which suggests that it is useful to consider the properties of collections of Pauli operators of the form $(g\mathcal{S})\cap\mathcal{B}$ with g an element of $\mathcal{W}$. The following result, proved in App. 6.A, turns out to be useful.

Lemma 6.2. *Let g, h be two arbitrary elements of $\mathcal{W}$, and $\mathcal{B}$ the collection of operators with base in B.*

i) The set $(g\mathcal{S})\cap\mathcal{B}$ is empty if and only if $(g^{-1}\mathcal{S})\cap\mathcal{B}$ is empty.

ii) Every nonempty set of the form $(g\mathcal{S})\cap\mathcal{B}$ contains precisely

$$M = |\mathcal{S}\cap\mathcal{B}| \geq 1 \tag{6.54}$$

elements.

iii) Two nonempty sets $(g\mathcal{S})\cap\mathcal{B}$ and $(h\mathcal{S})\cap\mathcal{B}$ are either identical, which means $g\mathcal{S} = h\mathcal{S}$ and $\Sigma[(g\mathcal{S})\cap\mathcal{B}] = \Sigma[(h\mathcal{S})\cap\mathcal{B}]$, or else they have no elements in common and the operators $\Sigma[(g\mathcal{S})\cap\mathcal{B}]$ and $\Sigma[(h\mathcal{S})\cap\mathcal{B}]$ are distinct.

iv) If both $(g\mathcal{S})\cap\mathcal{B}$ and $(h\mathcal{S})\cap\mathcal{B}$ are nonempty, their product as sets, including multiplicity, is given by

$$[(g\mathcal{S})\cap\mathcal{B}]\cdot[(h\mathcal{S})\cap\mathcal{B}] = M[(gh\mathcal{S})\cap\mathcal{B}]. \tag{6.55}$$

By (6.55) we mean the following. The product (on the left) of any operator from the collection $(g\mathcal{S})\cap\mathcal{B}$ with another operator from the collection $(h\mathcal{S})\cap\mathcal{B}$ belongs to the collection $(gh\mathcal{S})\cap\mathcal{B}$ (on the right), and every operator in $(gh\mathcal{S})\cap\mathcal{B}$ can be written as such a product in precisely M different ways.

We are now in a position to state and prove our central result:

6.5.2 Isomorphism theorem

Theorem 6.3 (Isomorphism)**.** *Let C be an additive graph code with information group $\mathcal{G}$, P the projector onto the coding space $\mathcal{H}_C$ and B be some subset of the carrier qudits. Then the collection $\mathcal{G}^B$ of members of $\mathcal{G}$ with nonzero partial trace down to B,* (6.52)*, is a subgroup of the information group $\mathcal{G}$, and the mapping $\hat{g} \to g_B$ in* (6.51) *carries $\mathcal{G}^B$ to an isomorphic group $\mathcal{G}_B$ of nonzero operators on $\mathcal{H}_B$. Furthermore,*

i) If $\hat{g}$ and $\hat{h}$ are any two elements of $\mathcal{G}^B$, then

$$\mathrm{Tr}_{\bar{B}}[\hat{g}\hat{h}] = \mathrm{Tr}_{\bar{B}}[\hat{g}]\,\mathrm{Tr}_{\bar{B}}[\hat{h}]/N \quad \textit{or} \quad (gh)_B = g_B h_B \tag{6.56}$$

ii) If $\hat{g} \neq \hat{h}$ are distinct elements of $\mathcal{G}^B$, $g_B \neq h_B$ are distinct elements of $\mathcal{G}_B$.

iii) The identity element

$$P_B := \mathrm{Tr}_{\bar{B}}[P]/N, \tag{6.57}$$

of $\mathcal{G}_B$ is a projector onto a subspace of $\mathcal{H}_B$ (possibly the whole space) with rank equal to $\mathrm{Tr}[P]/N = K/N$.

The normalization constant N is given as

$$N := |\mathcal{S}\cap\mathcal{B}|\cdot D^{|\bar{B}|}/|\mathcal{S}| \tag{6.58}$$

where $\mathcal{B}$ are the operators based in B.

Proof. The proof is a consequence of Lemma 6.2 and the following observations. The trace $\mathrm{Tr}_{\bar{B}}[\hat{g}]$ in (6.51) is, apart from a constant, the trace of $\Sigma[(g\mathcal{S})\cap\mathcal{B}]$, and is zero if $(g\mathcal{S})\cap\mathcal{B}$ is empty. If the collection $(g\mathcal{S})\cap\mathcal{B}$ is not empty, then by Lemma 6.1 it consists of a collection of linearly independent operators, and the trace of its sum cannot vanish. Thus there is a one-to-one, see part

(iii) of Lemma 6.2, correspondence between nonempty sets of the form $(g\mathcal{S}) \cap \mathcal{B}$ and the elements $\hat{g}$ in $\mathcal{G}^B$. Then (i) and (iv) of Lemma 6.2 imply both that $\mathcal{G}^B$ is a group, and also that the map from $\mathcal{G}^B$ to $\mathcal{G}_B$ is a homomorphism, whereas (ii) shows that this is actually an isomorphism: $g_B = h_B$ is only possible when $g\mathcal{S} = h\mathcal{S}$. That N in (6.58) is the correct normalization follows from (6.54), (6.55), and (6.48). □

A significant consequence of Theorem 6.3 is the following result on the presence and absence of information in the subset B, using the terminology of Sec. 6.2:

Theorem 6.4. *Let C be an additive graph code on n carrier qudits, with information group $\mathcal{G}$. Let B be a subset of the carrier qudits, $\mathcal{G}^B$ the corresponding subset information group, and $\mathcal{J}(\hat{g})$ the type of information corresponding to $\hat{g}$ (as defined in Sec. 6.2). Then*

i) The $\mathcal{J}(\hat{g})$ type of information is perfectly present in B if and only if $\hat{g} \in \mathcal{G}^B$.

ii) The $\mathcal{J}(\hat{g})$ type of information is absent from B if and only if $\hat{g}^k \notin \mathcal{G}^B$ for all integers k between 1 and $D-1$.

iii) All information is perfectly present in B if and only if $\mathcal{G}^B = \mathcal{G}$.

iv) All information is absent from B if and only if $\mathcal{G}^B$ consists entirely of scalar multiples of the identity element P of $\mathcal{G}$.

The proof of the theorem can be found in App. 6.B. Statement (iii) is useful because the check of whether there is a perfect quantum channel from the input to B involves a finite group $\mathcal{G}$; one does not have to consider all normal operators of the form (6.2). Statement (ii) deserves further comment. If D is prime then the order of any element of the Pauli group (apart from the identity) is D, see the remark following (6.9). The same is true of elements of the quotient group $\overline{\mathcal{G}}$, (6.41), and thus of members $\hat{g}$ of the isomorphic group $\mathcal{G}$. Consequently, for any k in the interval $1 < k < D$, there is some m such that $1 = km \mod D$, which means $\hat{g} = (\hat{g}^k)^m$. And since $\mathcal{G}^B$ is a group, $\hat{g}^k \in \mathcal{G}^B$ implies $\hat{g} \in \mathcal{G}^B$. Thus when D is prime, $\hat{g} \notin \mathcal{G}^B$ is equivalent to $\hat{g}^k \notin \mathcal{G}^B$ for all integers k between 1 and $D-1$, and the latter can be replaced by the former in statement (ii). However, when D is composite it is quite possible to have $\mathrm{Tr}_{\bar{B}}[\hat{g}] = 0$ but $\mathrm{Tr}_{\bar{B}}[\hat{g}^{k'}] \neq 0$ for some k' larger than 1 and less than D; see the example below. In this situation we can still say that $\mathcal{J}(\hat{g}^{k'})$ is perfectly present, but it is not true that $\mathcal{J}(\hat{g})$ is absent. One can regard the type $\mathcal{J}(\hat{g})$ as a *refinement* of $\mathcal{J}(\hat{g}^{k'})$, and as explained in Sec. 6.2, although the coarse-grained $\mathcal{J}(\hat{g}^{k'})$ information is perfectly present in B, the additional information associated with the refinement is not.

As an example, suppose $\hat{g}$ has a spectral decomposition

$$\hat{g} = J_0 + \mathrm{i}J_1 - J_2 - \mathrm{i}J_3, \tag{6.59}$$

with the J_j orthogonal projectors such that

$$\mathrm{Tr}_{\bar{B}}[J_0] = \mathrm{Tr}_{\bar{B}}[J_2] \neq \mathrm{Tr}_{\bar{B}}[J_1] = \mathrm{Tr}_{\bar{B}}[J_3]. \tag{6.60}$$

Then $\mathrm{Tr}_{\bar{B}}[\hat{g}] = 0$, whereas

$$\hat{g}^2 = (J_0 + J_2) - (J_1 + J_3), \tag{6.61}$$

and thus $\mathrm{Tr}_{\bar{B}}[\hat{g}^2] \neq 0$. Thus $\hat{g}^2$ is an element of $\mathcal{G}^B$, whereas $\hat{g}$ is not, and so the coarse grained $\mathcal{J}(\hat{g}^2)$ information corresponding to the decomposition on the right side of (6.61) is present in B, while the further refinement corresponding to the right side of (6.59) is not. Precisely this structure is produced by a graph code on two carriers of dimension $D = 4$, with graph state $|G\rangle = |++\rangle$, coding group $\mathcal{C} = \langle Z_1 Z_2 \rangle$, information group $\mathcal{G} = \langle X_1 P, Z_1 Z_2 P \rangle$, coding space projector

$$P = (I + X_1 X_2^3 + X_1^2 X_2^2 + X_1^3 X_2)/4, \tag{6.62}$$

and

$$\hat{g} = X_1 P = |\bar{0}\bar{0}\rangle\langle\bar{0}\bar{0}| + \mathrm{i}|\bar{1}\bar{2}\rangle\langle\bar{1}\bar{2}| - |\bar{2}\bar{0}\rangle\langle\bar{2}\bar{0}| - \mathrm{i}|\bar{3}\bar{2}\rangle\langle\bar{3}\bar{2}|, \tag{6.63}$$

where $|\bar{j}\rangle = Z^j|+\rangle$ are the eigenvectors of the X operator.

6.5.3 Information flow

At this point let us summarize how we think about information "flowing" from the input via the encoding operation into a subset B of the code carriers. At the input the information is represented by the quotient group $\overline{\mathcal{G}}_0 = \mathcal{W}_0/\mathcal{S}_0$, see (6.41), or more concretely by the isomorphic group $\mathcal{G}_0$ of operators generated by the cosets, as in (6.48). The encoding operation UW, see (6.36) and (6.38), maps $\overline{\mathcal{G}}_0$ to the analogous $\overline{\mathcal{G}} = \mathcal{W}/\mathcal{S}$ associated with the code C, and likewise $\mathcal{G}_0$ to the group of operators $\mathcal{G}$ acting on the coding space $\mathcal{H}_C$. Tracing away the complement $\bar{B}$ of B maps some of the $\hat{g}$ operators of $\mathcal{G}$ to zero, and the remainder form the subset information group $\mathcal{G}^B$. Applying the inverse UW map to $\mathcal{G}^B$ gives $\mathcal{G}_0^B$, a subgroup of $\mathcal{G}_0$ that tells us what types of information at the input (i.e. before the encoding) are available in the subset of carriers B. This is illustrated by various examples in the next section.

6.6 Examples

6.6.1 General principles

In this section we apply the principles developed earlier in the chapter to some simple $[[n, k, \delta]]_D$ additive graph codes, where n is the number of qudit carriers, each of dimension D, the dimension of the coding space $\mathcal{H}_C$ is $K = D^k$, and δ is the distance of the code; see Chapter 10 of [NC00] for a definition of δ. We shall be interested in the subset information group $\mathcal{G}^B$, (6.52), that represents the information about the input that is present in the subset B of carriers. Rather than discussing $\mathcal{G}^B$ or its traced down counterpart $\mathcal{G}_B$, it will often be simpler to use $\mathcal{G}_0^B$, the subset information group referred back to the channel input, see Sec. 6.5.3 above, and in this case we add an initial subscript 0 to operators: X_{01} means the X operator on the first qudit of the input. Since all three groups are isomorphic to one another, the choice of which to use in any discussion is a matter of convenience. (In the examples below for the sake of brevity we sometimes omit a term $\mathrm{e}^{\mathrm{i}\phi} I$ from the list of generators of $\mathcal{G}_0^B$.)

Before going further it is helpful to list some general principles of quantum information that apply to all codes, and which can simplify the analysis of particular examples, or give an intuitive explanation of why they work. In the following statements "information" always means information about the input which has been encoded in the coding space through some isometry.

1. If all information is perfectly present in B, then all information is absent from $\bar{B}$.

2. If all information is absent from $\bar{B}$ then all information is perfectly present in B.

3. If the information about some orthonormal basis (i.e., the type corresponding to this decomposition of the identity) is perfectly present in B, then the information about a mutually-unbiased basis is absent from $\bar{B}$.

4. If two types of information that are "sufficiently incompatible" are both perfectly present in B, then all information is perfectly present in B. In particular this is so when the two types are associated with mutually unbiased bases.

5. For a code of distance δ all information is absent from any B if $|B| < \delta$, and all information is perfectly present in B if $|B| > n - \delta$.

Items 1, 2, 3 and 4 correspond to the No Splitting, Somewhere, Exclusion and Presence theorems of [Gri07], which also gives weaker conditions for "sufficiently incompatible." The essential idea behind 5 is found in Sec. III A of [GBP97] [2].

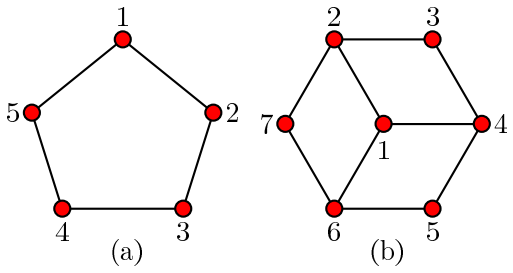

Figure 6.2: (a) The graph state for the $[[5,1,3]]_D$ code; (b) The graph state for Steane $[[7,1,3]]_2$ code

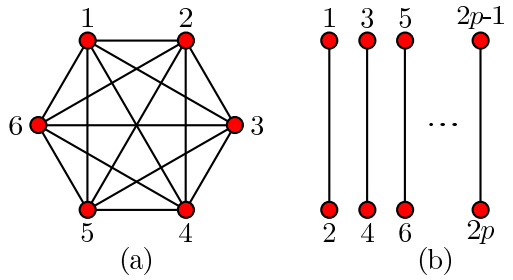

Figure 6.3: (a) Complete graph (on 6 qudits); (b) Bar graph with $n = 2p$ carriers and p bars

6.6.2 One encoded qudit

It was shown in [Rai99] that a $[[5,1,3]]_D$ code exists for all D. Here we consider the graph version [SW01] where the coding group is

$$\mathcal{C} = \langle Z_1 Z_2 Z_3 Z_4 Z_5 \rangle \tag{6.64}$$

and the graph state is shown in Fig. 6.2(a). Our formalism shows that, whatever the value of D, there are only two possibilities. When $|B|$ is 1 or 2 $\mathcal{G}^B$ is the just the group identity, the projector P on the coding space, so all information is absent whereas if $|B|$ is 3, 4 or (obviously) 5, $\mathcal{G}^B = \mathcal{G}$, so the subsystem B is the output of a perfect quantum channel. To be sure, these results also follow from principle 5 in the above list, given that $\delta = 3$ for this code.

The Steane $[[7,1,3]]_2$ code, a graphical version of which [YCO] has a coding group

$$\mathcal{C} = \langle Z_3 Z_5 Z_7 \rangle \tag{6.65}$$

for the graph state shown in Fig. 6.2 (b), is more interesting in that while principles 5 ensures that all $|B| \leq 2 = \delta - 1$ subsets of carriers contain zero information and all $|B| \geq 5 = n - \delta + 1$ subsets contain all the information, one qubit, it leaves open the question of what happens when $|B| = 3$ or 4. We find that all information is perfectly present when B is $\{1,2,5\}$, $\{1,3,6\}$, $\{1,4,7\}$, $\{2,3,4\}$, $\{2,6,7\}$, $\{4,5,6\}$, or $\{3,5,7\}$—representing three different symmetries in terms of the graph in the figure—and absent for all other cases of $|B| = 3$. Therefore all information is absent from the $|B| = 4$ subsets which are complements of the seven just listed, and perfectly present in all others of size $|B| = 4$. So far as we know, generalizations of this code to $D > 2$ have not been studied.

[2]It is shown in [GBP97] that if noise only affects a certain subset $\bar{B}$ of the carriers with $|\bar{B}| < \delta$, then the errors can be corrected using the complementary set B. In our notation this is equivalent to saying that all the information is in B.

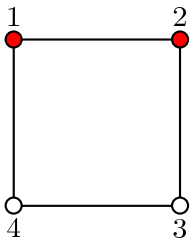

Figure 6.4: The graph state of the $[[4,2,2]]_D$ code

A simple code in which a specific type of information is singled out is $[[n,1,1]]_D$ generated by

$$\mathcal{C} = \langle Z_1 Z_2 \cdots Z_n \rangle \tag{6.66}$$

on the *complete graph*, illustrated in Fig. 6.3(a) for $n = 6$. Whereas all information is (of course) present when $|B| = n$, it turns out that for any subset B with $1 \leq |B| < n$ one has $\mathcal{G}_0^B = \langle X_{01} Z_{01} \rangle$, i.e., the abelian group consisting of all powers of the operator $X_1 Z_1$ on the input qudit. Thus the information is "classical," corresponding to that decomposition of the input identity that diagonalizes $X_1 Z_1$. The intuitive explanation for this situation is that this $X_1 Z_1$ type of information is separately copied as an ideal classical channel, see (6.6), to each of the carrier qudits, and as a consequence other mutually unbiased types of information are ruled out by principle 3. This, of course, is typical of "classical" information, which can always be copied.

A more interesting example in which distinct types of information come into play is the bar graph, Fig. 6.3 (b), in which n qudits are divided up into $p = n/2$ pairs or "bars," and the code is generated by

$$\mathcal{C} = \langle Z_1 Z_2 \cdots Z_n \rangle. \tag{6.67}$$

Let us say that a subset of carriers B has property I if the corresponding subgraph contains at least one of bars, and property II if it contains at least one qudit from each of the bars. Then:

(i) If B has property I but not II, $\mathcal{G}_0^B = \langle X_{01} \rangle$, an abelian group.

(ii) If B has property II but not I, $\mathcal{G}_0^B = \langle X_{01}^p Z_{01} \rangle$, another abelian group

(iii) If B has both property I and property II, all information (1 qudit) is perfectly present.

(iv) When B has neither property I nor II, all information is absent.

While both (i) and (ii) are "classical" in an appropriate sense and indeed represent an ideal classical channel, the two abelian groups do not commute with each other, so the two types of information are incompatible, and it is helpful to distinguish them. Case (iii) illustrates principle 4, since X_{01} and $X_{01}^p Z_{01}$ (whatever the value of p) correspond to mutually unbiased bases. In case (iv) the complement $\bar{B}$ of B possesses both properties I and II, and therefore contains all the information, so its absence from B is an illustration of principle 1.

6.6.3 Two encoded qudits

Consider a $[[4,2,2]]_D$ code based on the graph state shown in Fig. 6.4 whose coding group

$$\mathcal{C} = \langle Z_1 Z_2, Z_3 Z_4 \rangle, \tag{6.68}$$

employs two generators of order D, and thus encodes two qudits. Note that while the graph state has the symmetry of a square the coding group has a lower symmetry corresponding to the different types of nodes employed in the figure.

Let us begin with the qubit case $D = 2$. Our analysis shows that when $|B| = 1$ all information is absent, and thus for $|B| \geq 3$ all information is present, consistent with the fact that this code has

$\delta = 2$ [LYGG08], see principle 5. Thus the interesting cases are those in which $|B| = |\bar{B}| = 2$, for which one finds:

$$B = \{1,3\}, \bar{B} = \{2,4\}: \quad \mathcal{G}_0^B = \mathcal{G}_0^{\bar{B}} = \langle X_{01}Z_{01}Z_{02}, X_{01}X_{02}\rangle; \tag{6.69}$$

$$B = \{1,4\}, \bar{B} = \{2,3\}: \quad \mathcal{G}_0^B = \mathcal{G}_0^{\bar{B}} = \langle X_{01}Z_{01}, X_{02}Z_{02}\rangle; \tag{6.70}$$

$$B = \{1,2\}, \bar{B} = \{3,4\}: \quad \mathcal{G}_0^B = \mathcal{G}_0^{\bar{B}} = \langle X_{01}Z_{01}, X_{02}Z_{02}\rangle. \tag{6.71}$$

In each case the generators commute and thus the subgroup $\mathcal{G}_0^B$ is abelian. Hence the information is "classical", and the same type is present both in B and $\bar{B}$, not unlike the situation for the complete graph considered earlier. However, the three subgroups do not commute with each other, so the corresponding types of information are mutually incompatible, a situation similar to what we found for the bar graph.

For $D > 2$ it is again the case that all information is absent when $|B| = 1$ completely present for $|B| \geq 3$. And (6.69) and (6.70) remain correct (with each generator of order D), and these subgroups are again abelian. However, when $B = \{1,2\}$ and $\bar{B} = \{3,4\}$, (6.71) must be replaced with

$$\mathcal{G}_0^B = \langle Z_{01}X_{02}^2, Z_{02}\rangle, \quad \mathcal{G}_0^{\bar{B}} = \langle Z_{01}, X_{01}^2 Z_{02}\rangle. \tag{6.72}$$

In each case the two generators do not commute with each other, so neither subgroup is abelian. However, all elements of $\mathcal{G}_0^B$ commute with all elements of $\mathcal{G}_0^{\bar{B}}$. Also, the two subgroups are isomorphic (interchange subscripts 1 and 2).

For *odd* $D \geq 3$ one can use for $\mathcal{G}_0^B$ an alternative pair of generators

$$\mathcal{G}_0^B = \langle Z_{01}^m X_{02}, Z_{02}\rangle, \quad m := (D+1)/2, \tag{6.73}$$

whose order is D and whose commutator is

$$\big(Z_{01}^m X_{02}\big) Z_{02} = \omega Z_{02} \big(Z_{01}^m X_{02}\big). \tag{6.74}$$

This means—see (6.8)—that $\mathcal{G}_0^B$, and thus also the (isomorphic) $\mathcal{G}_0^{\bar{B}}$, is isomorphic to the Pauli group of a single qudit. Since $\mathcal{G}_0^B$ and $\mathcal{G}_0^{\bar{B}}$ commute with each other, it is natural to think of the pair as associated with the tensor product of two qudits with the same D. That this is correct can be confirmed by explicitly constructing a "pre-encoding" circuit embodying the unitary

$$(\mathrm{F}_1 \otimes \mathrm{F}_2)^\dagger \mathrm{CP}_{12}^{-m} (\mathrm{F}_1 \otimes \mathrm{F}_2), \tag{6.75}$$

expressed in terms of the Fourier and CP gates defined in Sec. 6.3.2, that carries the Pauli groups on "pre-input" qudits 1 and 2 onto $\mathcal{G}_0^B$ and $\mathcal{G}_0^{\bar{B}}$, respectively.

Things become more complicated for *even* $D \geq 4$, where $\mathcal{G}_0^B$ (and also $\mathcal{G}_0^{\bar{B}}$) are no longer isomorphic to the Pauli group of a single qudit.

6.7 Conclusion

We have shown that for additive graph codes with a set of n carrier qudits, each of the same dimension D, where D is any integer greater than 1, it is possible to give a precise characterization of the information from the coding space that is present in an arbitrary subset B of the carriers. This information corresponds to a subgroup $\mathcal{G}^B$ of a group $\mathcal{G}$, the information group of operators on the coding space, that spans the coding space and provides a useful representation of the information that it contains. We discuss how what we call a trivial code, essentially a tensor product of qudits of (possibly) different dimensions, can be encoded into the coding space in a manner which gives one a clear intuitive interpretation of $\mathcal{G}$. The subgroup $\mathcal{G}^B$ is then simply the subset of operators in $\mathcal{G}$ whose trace down to B is nonzero, and the traced-down operators when suitably normalized form

a group $\mathcal{G}_B$ that is isomorphic to $\mathcal{G}^B$. The information present in those operators in $\mathcal{G}$ that are not in $\mathcal{G}^B$ disappears so far as the subsystem B is concerned, as their partial traces are zero. This is the central result of our chapter and is illustrated by a number of simple examples in Sec. 6.6. We also provide in App. 6.C a relatively simple algorithm for finding the elements of $\mathcal{G}^B$.

These results can be extended to arbitrary qudit stabilizer codes even if they are not graph codes, by employing appropriate stabilizer and information groups, as in Sec. 6.4. Here, however, the concept of a trivial code, and thus our perspective on the encoding step, may not apply. The extension of these ideas, assuming it is even possible, to more general codes, such as nonadditive graph codes, remains an open question.

As shown in App. 6.D our formalism can be fitted within the general framework of invariant algebras as discussed in [BKK07a, BKK07b, Bén, BKNPV08]. The overall conceptual framework we use is somewhat different from that found in these references in that we directly address the question of what information is present in the subsystem of interest, rather than asking whether there exists some recovery operation (the $\mathcal{R}$ in App. 6.D) that will map an algebra of operators back onto its original space. Thus in our work the operator groups $\mathcal{G}^B$ on the coding space and $\mathcal{G}_B$ on the subsystem are isomorphic but not identical. Hence, even though there is, obviously, a close connection between our "group approach" and the "algebraic approach," the algebra of interest being generated from the group of operators, further relationships remain to be explored. The fact that the arguments in App. 6.D are not altogether straightforward suggests that the use of groups in cases where this is possible may provide a useful supplement, both mathematically and intuitively, to other algebraic ideas. In particular the additional structure present in an additive graph code allows one to determine $\mathcal{G}^B$ in $\mathcal{O}(n^\theta + K^2n^2)$, App. 6.C, as against $\mathcal{O}(K^6)$ for the algorithm presented in [BKNPV08] for a preserved matrix algebra, where K is the dimension of the input and output Hilbert space.

6.A Proof of Lemmas 6.1 and 6.2

Proof of Lemma 6.1

The operators in $p\mathcal{R}$ are linearly independent when those in $\mathcal{R}$ are linearly independent, since p is unitary and thus invertible. This establishes (i). For (ii), consider the case where q is the identity I. As the collection $\mathcal{R}$ is linearly independent, there is at most one $r \in \mathcal{R}$ such that pr is a multiple of the identity. If such an r exists, p is of the form $\mathrm{e}^{\mathrm{i}\phi}r^{-1}$, and since $\mathcal{R}$ is a group, $p\mathcal{R} = \mathrm{e}^{\mathrm{i}\phi}r^{-1}\mathcal{R} = \mathrm{e}^{\mathrm{i}\phi}\mathcal{R}$, we have situation ($\alpha$), with the collection $p\mathcal{R} \cup \mathcal{R}$ linearly dependent. Next assume the collection $p\mathcal{R} \cup \mathcal{R}$ is linearly dependent, which means there are complex numbers $\{a_r\}$ and $\{b_r\}$, not all zero, such that

$$\sum_{r\in\mathcal{R}} [a_r r + b_r pr] = 0. \tag{6.76}$$

This is not possible if all the a_r are zero, since this would mean $p\sum_r b_r r = 0$, thus $\sum_r b_r r = 0$ implying $b_r = 0$ for every r, since the $\mathcal{R}$ collection is by assumption linearly independent. Thus at least one a_r, say a_s is not zero. Multiply both sides of (6.76) by s^{-1} on the right and take the trace:

$$a_s \mathrm{Tr}[I] + \sum_{r\in\mathcal{R}} b_r \mathrm{Tr}[prs^{-1}] = 0, \tag{6.77}$$

implying there is at least one r for which $\mathrm{Tr}[prs^{-1}] \neq 0$. But then p is of the form $\mathrm{e}^{\mathrm{i}\phi}sr^{-1} = \mathrm{e}^{\mathrm{i}\phi}\bar{r}^{-1}$ for $\bar{r} = rs^{-1} \in \mathcal{R}$, so we are back to situation (α). Hence the alternative to (α) is (β): the operators in $p\mathcal{R} \cup \mathcal{R}$ are linearly independent. Finally, if q is not the identity I, simply apply the preceding argument with $\bar{p} = q^{-1}p$ in place of p.

Proof of Lemma 6.2

Statement (i) is a consequence of the fact that if an invertible operator is in $\mathcal{B}$, so is its inverse, and since $\mathcal{S}$ is a group, $g\mathcal{S}$ consists of the inverses of the elements in $g^{-1}\mathcal{S}$.

Statements (ii) and (iv) follow from a close examination of (6.55). Assume both sets on the left side are nonempty. If gs_1 and hs_2 are both in $\mathcal{B}$, so is their product $gs_1hs_2 = ghs_1s_2$, where we use the fact that g and h commute with every element of $\mathcal{S}$. If, on the other hand, $(gh\mathcal{S}) \cap \mathcal{B}$ and $(g\mathcal{S}) \cap \mathcal{B}$ are nonempty, any element, say ghs_1, in the former can be written using a specific element, say $g\bar{s}$, in the latter, as

$$ghs_1 = (g\bar{s})(hs_2) \tag{6.78}$$

where $s_2 = s_1\bar{s}^{-1}$ is uniquely determined by this equation, and the fact that both ghs_1 and $g\bar{s}$ are (by assumption) in $\mathcal{B}$ means the same is true of hs_2. Thus not only can every element of $(gh\mathcal{S}) \cap \mathcal{B}$ be written as a product of elements of $(g\mathcal{S}) \cap \mathcal{B}$, but there is a one-to-one correspondence between $(gh\mathcal{S}) \cap \mathcal{B}$ and $(g\mathcal{S}) \cap \mathcal{B}$, which must therefore be of equal size. A similar argument shows that $(gh\mathcal{S}) \cap \mathcal{B}$ and $(h\mathcal{S}) \cap \mathcal{B}$ are of the same size. This establishes both (ii) and (iv).

As for (iii), use the fact that the cosets $g\mathcal{S}$ and $h\mathcal{S}$ are either identical or have no elements in common, so the same is true of their intersections with $\mathcal{B}$. If $g\mathcal{S}$ and $h\mathcal{S}$ have no elements in common, Lemma 6.1 with $\mathcal{R} = \mathcal{S}$ tells us that either $g\mathcal{S} = \mathrm{e}^{\mathrm{i}\phi}(h\mathcal{S})$ for some nonzero ϕ, in which case $\Sigma[(g\mathcal{S}) \cap \mathcal{B}] = \mathrm{e}^{\mathrm{i}\phi}\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$ is distinct from $\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$, or else the collection $(g\mathcal{S}) \cup (h\mathcal{S})$ is linearly independent, which means that its intersection with $\mathcal{B}$ shares this property and the operators $\Sigma[(g\mathcal{S}) \cap \mathcal{B}]$ and $\Sigma[(h\mathcal{S}) \cap \mathcal{B}]$ are linearly independent.

6.B Proof of Theorem 6.4

The proof of Theorem 6.4 makes use of the following:

Lemma 6.5. *Let $\hat{g} = P\hat{g}P$ be an information operator in $\mathcal{G}$ with spectral decomposition*

$$\hat{g} = \sum_{j=0}^{m-1} \lambda_j J_j, \tag{6.79}$$

where the mutually orthogonal projectors J_j sum to P. Then each projector J_j can be written as a polynomial in $\hat{g}$ with $\hat{g}^0 = P$:

$$J_j = \sum_{k=0}^{m-1} \alpha_{jk}\hat{g}^k. \tag{6.80}$$

Proof. The proof consists in noting that

$$\hat{g}^k = \sum_{j=0}^{m-1} \lambda_j^k J_j = \sum_{j=0}^{m-1} \beta_{kj} J_j, \tag{6.81}$$

is a linear equation in the J_j with $\beta_{kj} = \lambda_j^k$ an $m \times m$ Vandermonde matrix whose determinant is $\prod_{j>k}(\mu_j - \mu_k)$ (see p. 29 of [HJ99]). As the μ_j are distinct the matrix β_{kj} has an inverse α_{jk}. □

To prove (i) of Theorem 6.4, first assume that $\hat{g}$ is in $\mathcal{G}^B$. Since $\mathcal{G}^B$ is a group with identity P, this means that all powers of $\hat{g}$, including $\hat{g}^0 = P$, are also in $\mathcal{G}^B$. Consequently, the projectors entering the spectral decomposition (6.79) of $\hat{g}$ satisfy

$$N^{-1}\mathrm{Tr}_{\bar{B}}[J_j]\ \mathrm{Tr}_{\bar{B}}[J_k] = \mathrm{Tr}_{\bar{B}}[J_jJ_k] = \delta_{jk}\mathrm{Tr}_{\bar{B}}[J_j], \tag{6.82}$$

with the first equality obtained by expanding J_j and J_k in powers of $\hat{g}$, (6.80), and using (6.56) along with the linearity of the partial trace. This orthogonality of the partial traces of different projectors,

see (6.3), implies that the $\mathcal{J}(\hat{g})$ type of information is perfectly present in B. Conversely, if the $\mathcal{J}(\hat{g})$ type of information is perfectly present in B then the partial traces down to B of the different J_j, which cannot be zero, are mutually orthogonal and thus linearly independent. Therefore by (6.79), $\mathrm{Tr}_{\bar{B}}[\hat{g}]$ cannot be zero, and $\hat{g}$ is in $\mathcal{G}^B$.

The prove (ii) note that $\hat{g}^k$ absent from $\mathcal{G}^B$ for $1 \leq k < D$ means that $\mathrm{Tr}_{\bar{B}}[\hat{g}^k] = 0$ for these values of k, and thus by taking the partial trace of both sides of (6.80) and using (6.57),

$$\mathrm{Tr}_{\bar{B}}[J_j] = N\alpha_{j0}P_B. \tag{6.83}$$

Since these partial traces are identical up to a multiplicative constant there is no information of the $\mathcal{J}(\hat{g})$ type in B. For the converse, if there is no $\mathcal{J}(\hat{g})$ information in B then there is also no $\mathcal{J}(\hat{g}^2)$, $\mathcal{J}(\hat{g}^3)$, etc. information in B, since the projectors which arise in the spectral decomposition of $\hat{g}^k$ are already in the spectral decomposition of $\hat{g}$, see (6.81). Consequently, by (i), these $\hat{g}^k$ must be absent from $\mathcal{G}^B$.

To prove (iii), note that if all information is perfectly present in B this means that for every $\hat{g} \in \mathcal{G}$ the $\mathcal{J}(\hat{g})$ information is present in B, and therefore, by (i), $\hat{g} \in \mathcal{G}^B$, so $\mathcal{G} = \mathcal{G}^B$. For the converse, let Q_1 and Q_2 be two orthogonal but otherwise arbitrary projection operators on subspaces of the coding space $\mathcal{H}_C$. Because the elements of the information group $\mathcal{G}$ form a basis for the set of linear operators on $\mathcal{H}_C$, see comments at the end of Sec. 6.4.3, Q_1 and Q_2 can both be written as sums of elements $\hat{g}$ in $\mathcal{G}$, and the same argument that was employed in (6.82) shows that the orthogonality of Q_1 and Q_2 implies the orthogonality of $\mathrm{Tr}_{\bar{B}}[Q_1]$ and $\mathrm{Tr}_{\bar{B}}[Q_2]$.

To prove (iv), note that if $\mathcal{G}^B$ consists entirely of scalar multiples of P, the partial trace down to B of any projector Q on a subspace of $\mathcal{H}_C$, since it can be written as a linear combination of the partial traces of the $\hat{g}$ in $\mathcal{G}$, most of which vanish, will be some multiple of P_B, and thus all information is absent from B. Conversely, if $\mathcal{G}^B$ contains a $\hat{g}$ which is not proportional to P the corresponding $\mathcal{J}(\hat{g})$ type of information will be present in B by (i), so it is not true that all information is absent from B, a contradiction.

6.C Algorithm for finding $\mathcal{G}^B$

Here we present an algorithm for determining the subset information group $\mathcal{G}^B$ by finding the elements $\hat{g}$ of $\mathcal{G}$ whose partial trace down to B is nonzero. If two or more elements differ only by a phase it is obviously only necessary to check one of them. For what follows it is helpful to adopt the abbreviation

$$E^{(\mathbf{x}|\mathbf{z})} := X^{\mathbf{x}}Z^{\mathbf{z}} \tag{6.84}$$

with $(\mathbf{x}|\mathbf{z})$ an n-tuple row vector pair, and thus a $2n$-tuple of integers between 0 and $D-1$. Arithmetic operations in the following analysis are assumed to be mod D.

First consider the trivial code on the trivial graph, Sec. 6.4.2, with information group $\mathcal{G}_0^B$ consisting of elements of the form $\hat{g}_0 = g_0P_0$, see (6.48), with $g_0 = E^{(\mathbf{x}_0|\mathbf{z}_0)}$ some element of $\mathcal{W}_0 = \langle \mathcal{S}_0^G, \mathcal{C}_0 \rangle$, and

$$P_0 = |\mathcal{S}_0|^{-1} \sum_{\mathbf{x}\in\mathcal{X}_0} X^{\mathbf{x}}, \tag{6.85}$$

where $\mathcal{X}_0$ denotes the collection of n-tuples that enter the stabilizer $\mathcal{S}_0$, (6.37). By choosing $\mathbf{x}_0$ and $\mathbf{z}_0$ to be of the form

$$\begin{aligned} \mathbf{x}_0 &= (\xi_1, \xi_2, \ldots \xi_k, 0, 0, \ldots 0), \\ \mathbf{z}_0 &= (\zeta_1 m_1, \zeta_2 m_2, \ldots \zeta_k m_k, 0, 0, \ldots 0), \end{aligned} \tag{6.86}$$

using integers in the range

$$0 \leq \xi_j \leq (d_j - 1), \quad 0 \leq \zeta_j \leq (d_j - 1), \tag{6.87}$$

we obtain a single representative $g_0 = E^{(\mathbf{x}_0|\mathbf{z}_0)}$ for each coset $g_0\mathcal{S}_0$ in $\mathcal{W}/\mathcal{S}_0$. The corresponding information operator, which depends only on the coset, is

$$\hat{g}_0 = E^{(\mathbf{x}_0|\mathbf{z}_0)}P_0 = |\mathcal{S}_0|^{-1} \sum_{\mathbf{x}\in\mathcal{X}_0} \omega^{-\mathbf{z}_0\mathbf{x}} E^{(\mathbf{x}+\mathbf{x}_0|\mathbf{z}_0)}, \tag{6.88}$$

where the addition of $\mathbf{x}$ and $\mathbf{x}_0$ is component-wise mod D, and $\mathbf{z}_0\mathbf{x}$ denotes the scalar product of $\mathbf{z}_0$ and $\mathbf{x}$ mod D (multiply corresponding components and take the sum mod D).

Elements of the information group $\mathcal{G}^B$ of the nontrivial code of interest to us are then of the form

$$\begin{aligned} \hat{g} &= (UW)\hat{g}_0(UW)^\dagger \\ &= |\mathcal{S}_0|^{-1} \sum_{\mathbf{x}\in\mathcal{X}_0} \omega^{\nu(\mathbf{x},\mathbf{x}_0,\mathbf{z})-\mathbf{z}_0\mathbf{x}} E^{(\mathbf{x}+\mathbf{x}_0|\mathbf{z}_0)Q}, \end{aligned} \tag{6.89}$$

where we use the fact that because the conjugating operator UW, (6.36), is a Clifford operator there is a $2n \times 2n$ matrix Q over $\mathbb{Z}_D^{2n}$, representing a symplectic automorphism [HDM05], such that

$$(UW)E^{(\mathbf{x}|\mathbf{z})}(UW)^\dagger = \omega^{\nu(\mathbf{x},\mathbf{z})}E^{(\mathbf{x}|\mathbf{z})Q}. \tag{6.90}$$

with $(\mathbf{x}|\mathbf{z})Q$ the $2n$-tuple, interpreted as an n-tuple pair, obtained by multiplying $(\mathbf{x}|\mathbf{z})$ on the right by Q, and $\nu(\mathbf{x},\mathbf{z})$ an integer whose value does not concern us. The explicit form of Q can be worked out by means of the encoding procedure presented in Sec. 6.4.2, using Tables 6.1 and 6.2.

The operators appearing in the sum on the right side of (6.89) are linearly independent Pauli products, since Q is nonsingular. The trace down to B of such a product is nonzero if and only if its base is in B, and when nonzero the result after the trace is essentially the same operator: see (6.53) and the associated discussion. Consequently $g_B = N^{-1}\mathrm{Tr}_{\bar{B}}[\hat{g}]$ is nonzero if and only if the trace down to B of at least one operator on the right side of (6.89) is nonzero. A useful test takes the form

$$\mathrm{Tr}_{\bar{B}}[E^{(\mathbf{x}|\mathbf{z})}] \neq 0 \Longleftrightarrow (\mathbf{x}|\mathbf{z})J = \mathbf{0}, \tag{6.91}$$

where $\mathbf{0}$ is the zero row vector, and J is a diagonal $2n \times 2n$ matrix with 1 at the diagonal positions j and $2j$ whenever qudit j belongs to $\bar{B}$, and 0 elsewhere. Therefore the $\hat{g}$ associated with $\mathbf{x}_0$ and $\mathbf{z}_0$ through (6.88) and (6.89) is a member of $\mathcal{G}^B$ if and only if there is at least one $\mathbf{x} \in \mathcal{X}_0$ such that

$$(\mathbf{x}+\mathbf{x}_0|\mathbf{z}_0)QJ = \mathbf{0} \quad \text{or} \quad (\mathbf{x}|\mathbf{0})QJ = -(\mathbf{x}_0|\mathbf{z}_0)QJ. \tag{6.92}$$

The $\mathbf{x}$ that belong to $\mathcal{X}_0$ are characterized by the equation

$$\mathbf{x}M = \mathbf{0}, \tag{6.93}$$

where M is an $n \times k$ matrix that is everywhere 0 except for $M_{jj} = m_j$ for $1 \leq j \leq k$, using the m_j that appear in (6.28). Consequently, instead of asking whether (6.92) has a solution $\mathbf{x}$ belonging to $\mathcal{X}_0$ one can just as well ask if there is any solution to the pair (6.92) and (6.93), or equivalently to the equation

$$\mathbf{x}T = \mathbf{u}_0 \tag{6.94}$$

where T is an $n \times (2n + k)$ matrix whose first $2n$ columns consist of the top half of the matrix QJ, (upper n elements of each column), and whose last k columns are the matrix M in (6.93); while $\mathbf{u}_0$ is a row vector whose first $2n$ elements are $-(\mathbf{x}_0|\mathbf{z}_0)QJ$ and last k elements are 0. Deciding if (6.94) has a solution $\mathbf{x}$ becomes straightforward once one has transformed T to Smith normal form, including determining the associated invertible matrices, see (6.32). As this needs to be done just once for a given additive code and a given subset B, the complexity of the algorithm for finding $\mathcal{G}^B$ is $\mathcal{O}(n^\theta)$ for finding the Smith form plus $\mathcal{O}(n^2K^2)$ for testing the K^2 elements of $\mathcal{G}$ once the Smith form is available. By using the group property of $\mathcal{G}^B$ one can construct a faster algorithm, but that is beyond the scope of this Dissertation.

6.D Correctable $*$-algebra

The counterpart in [BKK07b] of our notion of information perfectly present at the output of a quantum channel, see Sec. 6.2, is that of a *correctable $*$-algebra* $\mathcal{A}$ of operators acting on a Hilbert space. The $*$ (sometimes denoted C*) means that $\mathcal{A}$, as well as being an algebra of operators in the usual sense, contains $a^\dagger$ whenever it contains a. Let the channel superoperator $\mathcal{E}$ be represented by Kraus operators,

$$\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger, \tag{6.95}$$

satisfying the usual closure condition $\sum_j E_j^\dagger E_j = I$, and let P be a projector onto some subspace $P\mathcal{H}$ of the Hilbert space $\mathcal{H}$. Then a $*$-algebra $\mathcal{A}$ is defined in [BKK07b] to be *correctable for $\mathcal{E}$ on states in $P\mathcal{H}$* provided $a = PaP$ for every a in $\mathcal{A}$, and there exists a superoperator $\mathcal{R}$ (the recovery operation in an error correction scheme) whose domain is the range of $\mathcal{E}$, whose range is $\mathcal{L}(\mathcal{H})$, and such that

$$P[(\mathcal{R}\circ\mathcal{E})^\dagger(a)]P = a = PaP \tag{6.96}$$

for all $a \in \mathcal{A}$. Here the dagger denotes the adjoint of the superoperator in the sense that

$$\mathrm{Tr}\left[b\left((\mathcal{R}\circ\mathcal{E})(c)\right)\right] = \mathrm{Tr}\left[\left((\mathcal{R}\circ\mathcal{E})^\dagger(b)\right)c\right] \tag{6.97}$$

for any b and c in $\mathcal{L}(\mathcal{H})$. In [BKK07b], see Theorem 9 and Corollary 10, it is shown that any correctable algebra in this sense is a subalgebra of (what we call) a *maximal* correctable algebra

$$\mathcal{A}_M = \left\{ a \in \mathcal{L}(P\mathcal{H}) : [a, PE_i^\dagger E_j P] = 0 \quad \forall\, i,j \right\}. \tag{6.98}$$

We can apply this to our setting described in Secs. 6.4 and 6.5 where P is the projector on the coding space $\mathcal{H}_C$ and $\mathcal{E}_B$ is the superoperator for the partial trace down to the subset B of carriers,

$$\mathcal{E}_B(\rho) = \mathrm{Tr}_{\bar{B}}[\rho] = \sum_j E_j \rho E_j^\dagger \quad \text{for } \rho \in \mathcal{L}(\mathcal{H}) \tag{6.99}$$

with Kraus operators

$$E_j := I_B \otimes \langle j|_{\bar{B}}\,, \tag{6.100}$$

where $|j\rangle_{\bar{B}}$ is any orthonormal basis of $\mathcal{H}_{\bar{B}}$, so

$$E_i^\dagger E_j = I_B \otimes |i\rangle\langle j|_{\bar{B}}\,. \tag{6.101}$$

We shall now show that collection of operators in $\mathcal{G}^B$ (defined in Theorem 6.3) spans a $*$-algebra which is correctable for $\mathcal{E}_B$ on states in $P\mathcal{H} = \mathcal{H}_C$, and is the maximal algebra of this kind, i.e. $\mathrm{span}(\mathcal{G}^B) = \mathcal{A}_M$. First note that $\mathrm{span}(\mathcal{G}^B)$ is indeed a $*$-algebra: every $\hat{g} \in \mathcal{G}$ is a unitary operator and $\mathcal{G}$ contains the adjoint of each of its elements; replacing g with $g^\dagger$ in (6.48) yields $\hat{g}^\dagger$. Of course $\mathrm{Tr}_{\bar{B}}[\hat{g}] = 0$ if and only if $\mathrm{Tr}_{\bar{B}}[\hat{g}^\dagger] = 0$ and in addition, $a = PaP$ for $a \in \mathrm{span}(\mathcal{G}^B)$ because $\hat{g} = P\hat{g}P$, (6.48).

By definition $\mathrm{Tr}_{\bar{B}}[\hat{g}] \neq 0$ for $\hat{g} \in \mathcal{G}^B$, and this means that the partial trace down to B of at least one element in the corresponding coset $g\mathcal{S}$, see (6.48), must be nonzero. Let h be such an element; since it is a Pauli product it must be of the form $h = h_B \otimes I_{\bar{B}}$. As a consequence,

$$\begin{aligned}[\hat{g}, PE_i^\dagger E_j P] &= [\hat{h}, PE_i^\dagger E_j P] = P[h, E_i^\dagger E_j]P \\ &= P[\,h_B \otimes I_{\bar{B}}, I_B \otimes |i\rangle\langle j|_{\bar{B}}\,]P = 0,\end{aligned} \tag{6.102}$$

where the successive steps are justified as follows. Since $\hat{g}$ depends only on the coset $g\mathcal{S}$ and h belongs to this coset, $h\mathcal{S} = g\mathcal{S}$ and $\hat{h} = Ph = hP = \hat{g}$. This means we can move the projector P

outside the commutator bracket, and once outside it is obvious that the latter vanishes for every i and j. Thus any $\hat{g}$ in $\mathcal{G}^B$ belongs to the maximal $\mathcal{A}_M$ defined in (6.98), as do all linear combinations of the elements in $\mathcal{G}^B$.

To show that $\mathcal{A}_M$ is actually spanned by $\mathcal{G}^B$ we note that any a belonging to $\mathcal{A}_M$ can be written as

$$a = b + c, \tag{6.103}$$

where b is a linear combination of elements of $\mathcal{G}^B$ and c of elements of $\mathcal{G}$ that do not belong to $\mathcal{G}^B$, so $\mathrm{Tr}_{\bar{B}}[c] = \mathrm{Tr}_{\bar{B}}[c^\dagger] = 0$. Thus it is the case that

$$P(\mathcal{R} \circ \mathcal{E}_B)^\dagger(b)P = b, \quad P(\mathcal{R} \circ \mathcal{E}_B)^\dagger(c)P = c, \tag{6.104}$$

where the first follows, see (6.96), from the previous argument showing that the span of $\mathcal{G}^B$ is a subalgebra of $\mathcal{A}_M$, and the second from linearity and the assumption that a belongs to $\mathcal{A}_M$. Multiply the second equation by $c^\dagger$ and take the trace:

$$\begin{aligned} \mathrm{Tr}[c^\dagger c] &= \mathrm{Tr}\left[c^\dagger P\left((\mathcal{R} \circ \mathcal{E}_B)^\dagger(c)\right)P\right] \\ &= \mathrm{Tr}\left[\left(\mathcal{R} \circ \mathcal{E}_B(c^\dagger)\right)c\right] = 0, \end{aligned} \tag{6.105}$$

where we used the fact that $Pc^\dagger P = c^\dagger$, and $\mathcal{E}_B(c^\dagger) = \mathrm{Tr}_{\bar{B}}[c^\dagger] = 0$. Thus $c = 0$ and any element of $\mathcal{A}_M$ is a linear combination of the operators in $\mathcal{G}^B$.

In conclusion, we have shown for any additive graph code C and any subset of carrier qudits B, the $*$-algebra spanned by operators in $\mathcal{G}^B$ is exactly the maximal correctable algebra $\mathcal{A}_M$ defined in (6.98). In App. 6.C we outline an algorithm that enumerates the elements in $\mathcal{G}^B$ for any $\mathcal{H}_C$ and $\mathcal{E}_B$, which in light of the result above is an operator basis of $\mathcal{A}_M$.

7

Bipartite equientagled bases

7.1 Introduction

We present two different solutions to the problem posed by Karimipour and Memarzadeh in [KM06] of constructing an orthonormal basis of two qudits with the following properties: (i) The basis continuously changes from a product basis (every basis state is a product state) to a maximally entangled basis (every basis state is maximally entangled), by varying some parameter t, and (ii) for a fixed t, all basis states are equally entangled. As mentioned in [KM06], such a family of bases may find applications in various quantum information protocols including quantum cryptography, optimal Bell tests, investigation of the enhancement of channel capacity due to entanglement and the study of multipartite entanglement. For a more detailed motivation the interested reader may consult [KM06].

The chapter is organized as follows : In Sec. 7.2 we summarize the main results of [KM06] and then introduce the concept of Gauss sums and some useful related properties. Next we provide an explicit parameterization of a family of equientangled bases and we prove that it interpolates continuously between a product basis and a maximally entangled basis, for all dimensions. We illustrate the behaviour of our solution with explicit examples. In Sec. 7.3 we construct another such family using a completely different method based on graph states, describe a simple extension of it to multipartite systems, and then illustrate its behaviour with specific examples. Finally in Sec. 7.4 we compare the two solutions and make some concluding remarks.

7.2 Construction based on Gauss sums

7.2.1 Summary of previous work

Let us start by summarizing the main results of [KM06]. Consider a bipartite Hilbert space $\mathcal{H} \otimes \mathcal{H}$, where both Hilbert spaces have the same dimension D. The authors first defined an arbitrary normalized bipartite state

$$|\psi_{0,0}\rangle = \sum_{k=0}^{D-1} a_k |k\rangle|k\rangle. \tag{7.1}$$

Next for $m, n = 0, 1, \ldots, D-1$, they considered the collection of D^2 "shifted" states

$$\begin{aligned} |\psi_{m,n}\rangle &= X^m \otimes X^{m+n} |\psi_{0,0}\rangle \\ &= \sum_{k=0}^{D-1} a_k |k \oplus m\rangle|k \oplus m \oplus n\rangle, \end{aligned} \tag{7.2}$$

where

$$X := \sum_{k=0}^{D-1} |k \oplus 1\rangle \langle k| \tag{7.3}$$

is the generalized Pauli (or shift) operator and $\oplus$ denotes addition modulo D. They noted that all states have the same value of entropy of entanglement [NC00] given by the von-Neumann entropy

$$E(|\psi_{m,n}\rangle) = E(|\psi_{0,0}\rangle) = -\sum_{k=0}^{D-1} |a_k|^2 \log_D |a_k|^2, \tag{7.4}$$

where the logarithm is taken in base D for normalization reasons so that all maximally entangled states have entanglement equal to one regardless of D.

Demanding the states in (7.2) be orthonormal yields

$$\sum_{k=0}^{D-1} (a_k)^* a_{k\oplus m} = \delta_{m,0}, \ \forall m = 0, \ldots, D-1, \tag{7.5}$$

and the authors proved (see their Eqn. (36)) that (7.5) is satisfied if and only if the coefficients a_k have the form

$$a_k = \frac{1}{D} \sum_{j=0}^{D-1} \mathrm{e}^{\mathrm{i}\theta_j} \omega^{kj}, \tag{7.6}$$

where θ_j are arbitrary real parameters and $\omega = \mathrm{e}^{2\pi \mathrm{i}/D}$ is the D-th root of unity.

Therefore the authors found a family of D^2 orthonormal states, all having the same Schmidt coefficients and hence the same value of entanglement. To ensure it interpolates from a product basis to a maximally entangled basis, it is sufficient to find a set of parameters $\{\theta_j^0\}_{j=0}^{D-1}$ for which the magnitude of a_k is $|a_k| = 1/\sqrt{D}$ for all k. Then the problem is solved by defining

$$a_k(t) := \frac{1}{D} \sum_{j=0}^{D-1} \mathrm{e}^{\mathrm{i}t\theta_j^0} \omega^{kj}, \tag{7.7}$$

where $t \in [0, 1]$ is a real parameter. When $t = 0$ we have $a_k = \delta_{k,0}$ so the basis states are product states and when $t = 1$, the basis is maximally entangled by assumption. We also observe there is a continuous variation in between these two extremes as a function of t.

Karimipour and Memarzadeh considered the existence of such a set $\{\theta_j^0\}_{j=0}^{D-1}$ in arbitrary dimensions (see the last paragraph of Sec. V in [KM06]). They found particular solutions for $D \leqslant 5$, but did not find a general solution for arbitrary D.

7.2.2 Quadratic Gauss Sums

We now define the basic mathematical tools we will make use of in the rest of this section. The most important concept is that of a *quadratic Gauss sum*, defined below.

Quadratic Gauss Sums. *Let p, m be positive integers. The quadratic Gauss sum is defined as*

$$\sum_{j=0}^{p-1} \mathrm{e}^{2\pi \mathrm{i} j^2 m/p}. \tag{7.8}$$

The quadratic Gauss sums satisfy a reciprocity relation known as

Landsberg-Schaar Identity. *Let p, m be positive integers. Then*

$$\frac{1}{\sqrt{p}}\sum_{j=0}^{p-1} \mathrm{e}^{2\pi \mathrm{i} j^2 m/p} = \frac{\mathrm{e}^{\pi \mathrm{i}/4}}{\sqrt{2m}} \sum_{j=0}^{2m-1} \mathrm{e}^{-\pi \mathrm{i} j^2 p/2m} \tag{7.9}$$

The quadratic Gauss sums can be generalized as follows.

Generalized Quadratic Gauss Sums. *Let p, m, n be positive integers. The generalized quadratic Gauss sum is defined as*

$$\sum_{j=0}^{p-1} \mathrm{e}^{2\pi \mathrm{i}(j^2 m + jn)/p}. \tag{7.10}$$

Finally the following reciprocity formula for generalized Gauss sums holds.

Reciprocity Formula for Generalized Quadratic Gauss Sums. *Let p, m, n be positive integers such that $mp \neq 0$ and $mp + n$ is even. Then*

$$\frac{1}{\sqrt{p}}\sum_{j=0}^{p-1} \mathrm{e}^{\pi \mathrm{i}(j^2 m + jn)/p} = \mathrm{e}^{\pi \mathrm{i}(mp - n^2)/4mp} \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \mathrm{e}^{-\pi \mathrm{i}(j^2 p + jn)/m}. \tag{7.11}$$

The definitions of the Gauss sums (7.8) and (7.10) as well as the Landsberg-Schaar's identity (7.9) can be found in standard number theory books [HW08, EW05, Nat00]. The reciprocity formula for the generalized quadratic Gauss sum is not as well-known, and can be found in [BE81].

7.2.3 Explicit Solution

We now show that a family of equientangled bases that interpolates continuously between the product basis and the maximally entangled basis exists for all dimensions D, as summarized by the following Theorem.

Theorem 7.1. *The collection of D^2 normalized states*

$$|\psi_{m,n}(t)\rangle = \sum_{k=0}^{D-1} a_k(t) |k \oplus m\rangle |k \oplus m \oplus n\rangle, \tag{7.12}$$
$$m, n = 0, \ldots, D-1,$$

indexed by a real parameter $t \in [0, 1]$ with

$$a_k(t) = \frac{1}{D}\sum_{j=0}^{D-1} \mathrm{e}^{\mathrm{i}t\theta_j^0} \omega^{kj}, \qquad \omega = \mathrm{e}^{2\pi \mathrm{i}/D}, \tag{7.13}$$

with the particular choice of

$$\theta_j^0 = \begin{cases} \pi j^2/D & \text{if } D \text{ is even} \\ 2\pi j^2/D & \text{if } D \text{ is odd,} \end{cases} \tag{7.14}$$

defines a family of equientangled bases that continuously interpolates between a product basis at $t = 0$ and a maximally entangled basis at $t = 1$.

That (7.12) defines a family of equientangled bases that consists of a product basis at $t = 0$ follows directly from the remarks of Sec. 7.1, $a_k(0) = \delta_{k,0}$. Next note that a continuous variation of t in the interval $[0, 1]$ corresponds to a continuous variation of the Schmidt coefficients of the states in the basis. The latter implies that no matter which measure one uses to quantify the entanglement,

the measure will vary continuously with t, since any pure state entanglement measure depends only on the Schmidt coefficients of the state [Vid99].

The only thing left to show is that the basis states in Theorem 7.1 are maximally entangled when $t = 1$, or, equivalently, that $|a_k(1)| = 1/\sqrt{D}$ for all k. We prove this by explicitly evaluating the value of $a_k(1)$ in the following Lemma.

Lemma 7.2. *Let $a_k(t)$ and $\{\theta_j^0\}_{j=0}^{D-1}$ be as defined by Theorem 7.1. Then for all k*

$$a_k(1) = \frac{\mathrm{e}^{\pi \mathrm{i}/4}}{\sqrt{D}} \times \begin{cases} \omega^{-k^2/2}, & \text{if } D \text{ is even} \\ \omega^{-k^2/4}\left(\frac{1-\mathrm{i}^{2k+D}}{\sqrt{2}}\right), & \text{if } D \text{ is odd} \end{cases}. \tag{7.15}$$

Lemma 7.2 implies at once that $|a_k(1)| = 1/\sqrt{D}$, and therefore proves Theorem 7.1.

Proof. (of Lemma 7.2) Note first that the expression for $a_k(1)$ in (7.13) with θ_j^0 defined in (7.14) resembles the generalized quadratic Gauss sum (7.10). We will use the reciprocity formula (7.11) to prove Lemma 7.2. There are two cases to be considered: Even D and odd D.

Even D. Note that one can rewrite $a_k(1)$ in (7.13) with θ_j^0 defined in (7.14) as

$$a_k(1) = \frac{1}{D}\sum_{j=0}^{D-1} \mathrm{e}^{\pi \mathrm{i} j^2/D}\, \mathrm{e}^{2\pi \mathrm{i} jk/D} = \frac{1}{D}\sum_{j=0}^{D-1} \mathrm{e}^{\pi \mathrm{i}(j^2+2kj)/D}. \tag{7.16}$$

Applying the reciprocity formula (7.11) to last term in (7.16) with $m = 1, n = 2k, p = D$ (noting that $mp + n = D + 2k$ is even) yields

$$\begin{aligned} a_k(1) &= \frac{1}{\sqrt{D}}\mathrm{e}^{\pi \mathrm{i}(D-4k^2)/4D} = \frac{\mathrm{e}^{\pi \mathrm{i}/4}}{\sqrt{D}}(-1)^D \mathrm{e}^{-\pi \mathrm{i} k^2/D} \\ &= \frac{\mathrm{e}^{\pi \mathrm{i}/4}}{\sqrt{D}}\omega^{-k^2/2}, \text{ since } (-1)^D = 1 \text{ for even } D. \end{aligned} \tag{7.17}$$

Odd D. The proof is essentially the same as in the even D case, but we explicitly write it below for the sake of completeness. Using a similar argument we rewrite $a_k(1)$ in (7.13) with θ_j^0 defined in (7.14) as

$$a_k(1) = \frac{1}{D}\sum_{j=0}^{D-1} \mathrm{e}^{2\pi \mathrm{i} j^2/D}\, \mathrm{e}^{2\pi \mathrm{i} jk/D} = \frac{1}{D}\sum_{j=0}^{D-1} \mathrm{e}^{\pi \mathrm{i}(2j^2+2kj)/D}. \tag{7.18}$$

Applying again the reciprocity formula (7.11) to last term in (7.18) with $m = 2, n = 2k, p = D$ (noting that $mp + n = 2D + 2k$ is even) yields

$$\begin{aligned} a_k(1) &= \frac{1}{\sqrt{D}}\frac{\mathrm{e}^{\pi \mathrm{i}(2D-4k^2)/8D}}{\sqrt{2}}(1 + \mathrm{e}^{-\pi \mathrm{i}(D+2k)/2}) \\ &= \frac{\mathrm{e}^{\pi \mathrm{i}/4}}{\sqrt{D}}\omega^{-k^2/4}\left(\frac{1-\mathrm{i}^{2k+D}}{\sqrt{2}}\right), \end{aligned} \tag{7.19}$$

where we used $(-\mathrm{i})^{2k+D} = -(\mathrm{i}^{2k+D})$ since $2k + D$ is odd. This concludes the proof of Lemma 7.2 and implicitly of Theorem 7.1. ∎

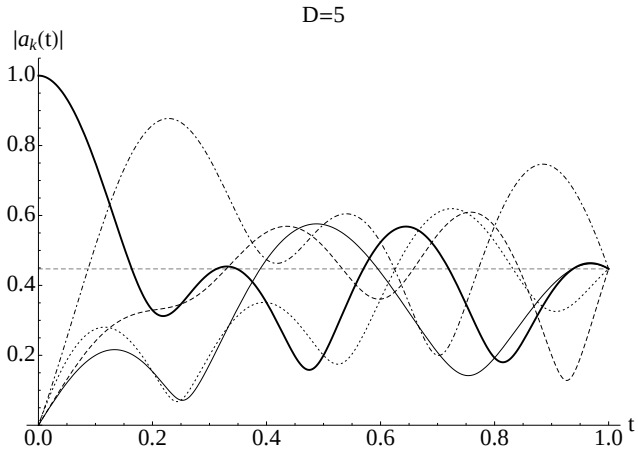

Figure 7.1: The variation of $|a_k(t)|$ with t for $D = 5$. Note how at $t = 0$ all coefficients but one are zero, and how at $t = 1$ all coefficients are equal in magnitude to $1/\sqrt{5}$, with a continuous variation in between. The dashed line represents the $1/\sqrt{5}$ constant function.

7.2.4 Examples

In this section we present some examples that illustrate the behaviour of the solution we provided in Theorem 7.1, for various dimensions. First we consider $D = 5$ and we plot the absolute values of the $a_k(t)$ coefficients as a function of t in Fig. 7.1. It is easy to see that indeed the basis interpolates between a product basis and a maximally entangled one in a continuous manner. We observe that all coefficients are non-zero for $t > 0$ and we believe that this is probably also the case for all odd D's.

In Fig. 7.2 we perform the same analysis as above, but now for $D = 8$. We observed that some coefficients vanish for some values of t, which seems to be true in general for even D.

In Fig. 7.3 we plot the entropy of entanglement of the states in the basis as a function of t for dimensions $D = 2, 3, 5, 8$ and 100. We see how the entanglement varies continuously but not monotonically between 0 and 1.

Finally in Fig. 7.4 we display a parametric plot of the variation of the second Schmidt coefficient $a_1(t)$ in the complex plane as t is varied from 0 to 1 for $D = 51$, so that the reader can get an idea of how the coefficients defined in (7.13) look in general. The other coefficients a_k look similar.

7.3 Construction based on Graph States

7.3.1 Explicit solution

We provide below another solution to the problem that uses qudit graph states. Again having in mind a bipartite Hilbert space $\mathcal{H} \otimes \mathcal{H}$, both local spaces having dimension D, we define a one-qudit state

$$|+\rangle := \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} |k\rangle. \tag{7.20}$$

It is easy to see that the collection of D states

$$|\overline{m}\rangle := Z^m |+\rangle, \quad m = 0, \ldots, D-1 \tag{7.21}$$

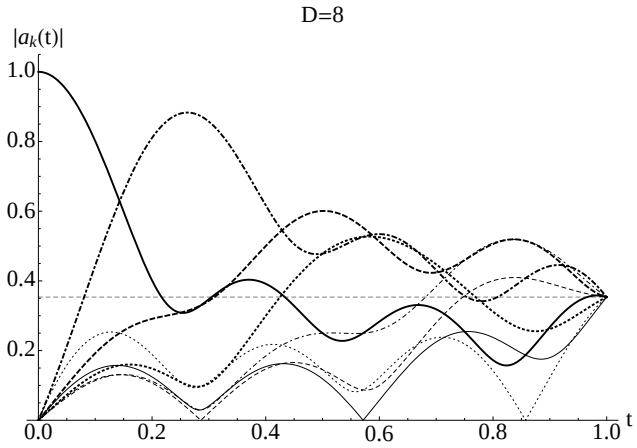

Figure 7.2: The variation of $|a_k(t)|$ with t for $D = 8$. Again note how at $t = 0$ all coefficients but one are zero, and how at $t = 1$ all coefficients are equal in magnitude to $1/\sqrt{8}$, with a continuous variation in between. The dashed line represents the $1/\sqrt{8}$ constant function.

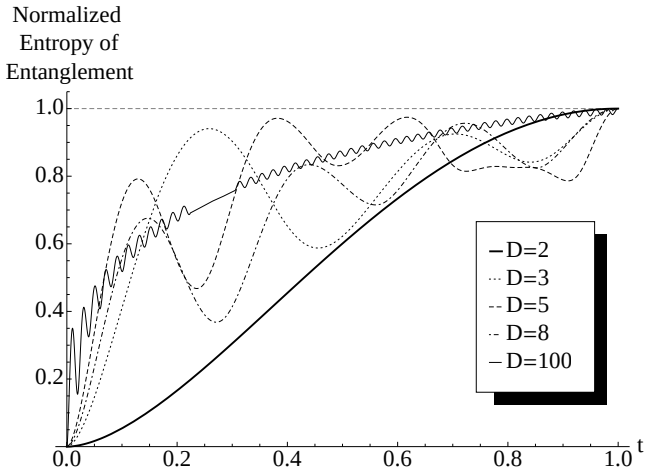

Figure 7.3: The entropy of entanglement as a function of t for various dimensions. Note that the variation is not monotonic (except for $D = 2$), although for large D the oscillations tend to be smoothed out.

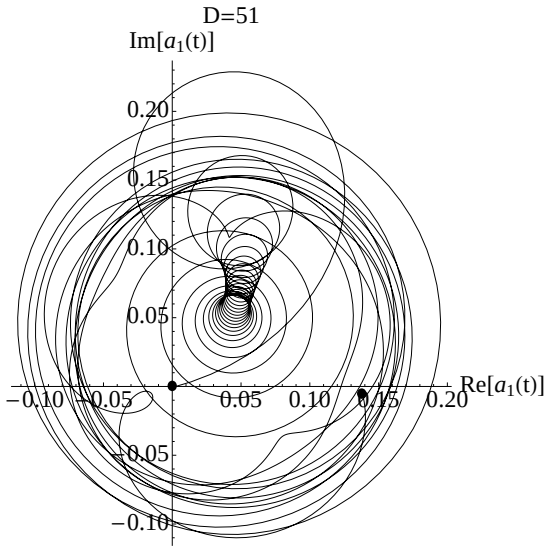

Figure 7.4: Parametric plot of $a_1(t)$ in the complex plane as t is varied from 0 to 1. Note that $a_1(0) = 0$ and $a_1(1) = \frac{1-\mathrm{i}}{\sqrt{2\cdot 51}}\mathrm{e}^{\pi\mathrm{i}(\frac{1}{4}-\frac{1}{2\cdot 51})}$, the value provided by Lemma 7.2. The starting point $t = 0$ and the ending point $t = 1$ are marked by solid disks.

defines an orthonormal basis of $\mathcal{H}$ (also known as the Fourier basis), $\langle\overline{m}|\overline{n}\rangle = \delta_{mn}$, where

$$Z := \sum_{k=0}^{D-1} \omega^k |k\rangle \langle k| \,, \tag{7.22}$$

with $\omega = \mathrm{e}^{2\pi\mathrm{i}/D}$ being the D-th root of unity. It then follows at once that the collection of D^2 states

$$|\overline{m}\rangle|\overline{n}\rangle = (Z^m \otimes Z^n)|+\rangle|+\rangle, \quad m, n = 0, \ldots, D-1 \tag{7.23}$$

defines an orthonormal product basis of the bipartite Hilbert space $\mathcal{H} \otimes \mathcal{H}$.

Next we define the generalized controlled-Phase gate as

$$C := \sum_{k=0}^{D-1} |k\rangle \langle k| \otimes Z^k = \sum_{j,k=0}^{D-1} \omega^{jk} |j\rangle \langle j| \otimes |k\rangle \langle k| \tag{7.24}$$

and note that C is a unitary operator that commutes with $Z^m \otimes Z^n$, for all $m, n = 0, \ldots, D-1$. The state

$$|G\rangle := C|+\rangle|+\rangle = \frac{1}{D} \sum_{j,k=0}^{D-1} \omega^{jk} |j\rangle|k\rangle \tag{7.25}$$

is an example of a two-qudit *graph state* and it is not hard to see that $|G\rangle$ is maximally entangled. Then the collection of D^2 states

$$\begin{aligned} (Z^m \otimes Z^n)|G\rangle &= (Z^m \otimes Z^n)C|+\rangle|+\rangle \\ &= C(Z^m \otimes Z^n)|+\rangle|+\rangle, \quad m, n = 0, \ldots, D-1 \end{aligned} \tag{7.26}$$

defines an orthonormal basis of the bipartite Hilbert space $\mathcal{H} \otimes \mathcal{H}$, which we call a *graph basis*. Since $Z^m \otimes Z^n$ are local unitaries and $|G\rangle$ is a maximally entangled state, then all the other graph basis

states must also be maximally entangled. For more details about graph states of arbitrary dimension see [HDE+, LYGG08, GLG10].

We now have all the tools to construct a continuous interpolating family of equientangled bases, as summarized by the Theorem below.

Theorem 7.3. *The collection of D^2 normalized states*

$$|G_{m,n}(t)\rangle = (Z^m \otimes Z^n)C(t)|+\rangle|+\rangle, \qquad m,n = 0,\ldots,D-1, \tag{7.27}$$

indexed by a real parameter $t \in [0,1]$ where

$$C(t) = \sum_{j,k} \omega^{jkt} |j\rangle\langle j| \otimes |k\rangle\langle k| \tag{7.28}$$

defines a family of equientangled bases that continuously interpolates between a product basis at $t = 0$ and a maximally entangled basis at $t = 1$.

Proof. We make the crucial observation that $C(t)$ commutes with $Z^m \otimes Z^n$ for all $m,n = 0,\ldots,D-1$ and all $t \in [0,1]$ which implies that $\{|G_{m,n}(t)\rangle\}_{m,n=0}^{D-1}$ defines an orthonormal basis since it differs from the orthonormal basis in (7.23) only by the unitary operator $C(t)$. All states in the basis are equally entangled, and moreover, share the same set of Schmidt coefficients since any two basis states are equivalent up to local unitaries of the form $Z^m \otimes Z^n$.

Finally note that $C(t=0) = I \otimes I$ and $C(t=1) = C$ (defined in (7.24)), and therefore at $t = 0$ the basis is product, see (7.23), and at $t = 1$ the basis is maximally entangled, see (7.26). The operator $C(t)$ can be viewed as a controlled-Phase gate whose "entangling strength" can be tuned continuously. The Schmidt coefficients of the states in the basis vary continuously with t and hence the entanglement also varies continuously with t, regardless of which entanglement measure one uses (see the remarks following Theorem 7.1). □

Our construction above can be expressed in the framework described in the last two paragraphs of Sec. II of [KM06], by setting $U_m = Z^m$ and $V_n = Z^n$.

Next we prove that the Schmidt coefficients of the basis states in Theorem 7.3 are all non-zero for any $t > 0$, so all bases consist of full Schmidt rank states whenever $t > 0$.

Lemma 7.4. *The equientangled family of bases $\{|G_{m,n}(t)\rangle\}_{m,n=0}^{D-1}$ defined in Theorem 7.3 consists of full Schmidt rank states, for any $0 < t \leqslant 1$.*

Proof. We will show that the product of the Schmidt coefficients is always non-zero, which implies that no Schmidt coefficient can be zero, whenever $0 < t \leqslant 1$.

Let

$$|\psi\rangle = \sum_{j,k=0}^{D-1} \Omega_{jk}|j\rangle|k\rangle \tag{7.29}$$

be an arbitrary normalized pure state in a bipartite Hilbert space $\mathcal{H}\otimes\mathcal{H}$ and let $\{\lambda_k\}$ denote the set of Schmidt coefficients of $|\psi\rangle$ satisfying $\sum_k \lambda_k = 1$; note that they are equal to the squares of the singular values of the coefficient matrix Ω in (7.29). The product of the squares of the singular values is just the product of the eigenvalues of $\Omega\Omega^\dagger$, the latter product being equal to $\det(\Omega\Omega^\dagger) = |\det(\Omega)|^2$, so we conclude that

$$\prod_{k=0}^{D-1} \lambda_k = |\det(\Omega)|^2. \tag{7.30}$$

The states $|G_{m,n}(t)\rangle$ of Theorem 7.3 share the same set of Schmidt coefficients (they are all related by local unitaries) so it suffices to show that the product of the Schmidt coefficients is non-zero only for the state $|G_{0,0}(t)\rangle$. Recall that

$$|G_{0,0}(t)\rangle = C(t)|+\rangle|+\rangle = \sum_{j,k} \frac{\omega^{jkt}}{D}|j\rangle|k\rangle. \tag{7.31}$$

Expressing the coefficients ω^{jkt}/D as a matrix $\Omega(t)$, one can easily see that $D \cdot \Omega(t)$ is a $D \times D$ Vandermonde matrix whose determinant is

$$\det\left[D \cdot \Omega(t)\right] = \prod_{j>k}(\omega^{jt} - \omega^{kt}) = \prod_{j>k} \omega^{kt}\left[\omega^{(j-k)t} - 1\right] \tag{7.32}$$

(see p. 29 of [HJ99] for more details on Vandermonde matrices). For a given t, the product above is zero if and only if at least one term is zero, i.e. there must exist integers j, k, with $0 \leqslant k < j \leqslant D-1$, such that

$$(j-k)t = nD \Longleftrightarrow t = n\frac{D}{j-k}, \tag{7.33}$$

for some positive integer $n \geqslant 0$. Note that $0 < j - k \leqslant D - 1$, so $D/(j-k) > 1$ and the above equation can never be satisfied for $0 < t \leqslant 1$. We have therefore proved that $\det[\Omega(t)] \neq 0$ for $0 < t \leqslant 1$, which, in the light of (7.30), is equivalent to saying that the product of the Schmidt coefficients is non-zero for $0 < t \leqslant 1$, and this concludes the proof of the Lemma. □

For this family of equientangled bases, we do not have an analytic expression for the Schmidt coefficients nor the entropy of entanglement for general D though they can be easily found by numerically diagonalizing the coefficient matrix $\Omega(t)\Omega(t)^\dagger$. Having said that, we derived a simple analytic expression for the *product* of all Schmidt coefficients, see (7.30) and (7.32), which is simply related to an entanglement monotone called G-concurrence (first introduced in [Gou05]) which is defined for a pure bipartite state (7.29) in terms of its Schmidt coefficients $\{\lambda_k\}$ as

$$C_G(|\psi\rangle) = D\left(\prod_{k=0}^{D-1}\lambda_k\right)^{1/D} = D|\det(\Omega)|^{2/D} \tag{7.34}$$

where $\sum_k \lambda_k = 1$. The G-concurrence is zero whenever at least one Schmidt coefficient is zero and is equal to one if and only if the state is maximally entangled. Unlike the entropy of entanglement, we are able to show two analytical results that are true for all D expressed in Lemmas 7.5 and 7.6.

Lemma 7.5. *The G-concurrence of the equientangled basis states, $\{|G_{m,n}(t)\rangle\}_{m,n=0}^{D-1}$ defined in Theorem 7.3 is*

$$C_G(t) = \frac{2^{D-1}}{D}\prod_{r=1}^{D-1}\left[\sin^2(\pi r t/D)\right]^{(D-r)/D} \text{ for all } m, n, D. \tag{7.35}$$

Proof. Every basis state has the same G-concurrence since they all share the same set of Schmidt coefficients (recall that they differ only by local unitaries). Invoking the definition of G-concurrence,

we have

$$C_G(t) = D|\det(\Omega(t))|^{2/D} = D\left|\frac{1}{D^D}\det(D\cdot\Omega(t))\right|^{2/D} \tag{7.36}$$

$$= \frac{1}{D}\prod_{j>k}\left|\omega^{(j-k)t}-1\right|^{2/D} = \frac{1}{D}\prod_{r=1}^{D-1}\left|\omega^{rt}-1\right|^{\frac{2(D-r)}{D}} \tag{7.37}$$

$$= \frac{1}{D}\prod_{r=1}^{D-1}\left[2-2\frac{\omega^{rt}+\omega^{-rt}}{2}\right]^{\frac{D-r}{D}} \tag{7.38}$$

$$= \frac{1}{D}\prod_{r=1}^{D-1}2^{(D-r)/D}\left[1-\cos(2\pi rt/D)\right]^{\frac{D-r}{D}} \tag{7.39}$$

$$= \frac{1}{D}\prod_{r=1}^{D-1}2^{2(D-r)/D}\left[\sin^2(\pi rt/D)\right]^{\frac{D-r}{D}} \tag{7.40}$$

$$= \frac{2^{D-1}}{D}\prod_{r=1}^{D-1}\left[\sin^2(\pi rt/D)\right]^{(D-r)/D}, \tag{7.41}$$

where in (7.36) we used the fact that $\det(cM) = c^D\det(M)$ for a $D\times D$ arbitrary matrix M and an arbitrary constant c. The first equality in (7.37) follows at once from (7.32), whereas the second equality in (7.37) follows from a simple counting argument in which one replaces $j-k$ by r, making sure that the different pairs (j,k), $j>k$, that give rise to the same r are counted; for a given r there are $D-r$ such pairs. □

It turns out that the G-concurrence has the following nice property:

Lemma 7.6. *The G-concurrence of the basis states $\{|G_{m,n}(t))\}_{m,n=0}^{D-1}$ in (7.35) is strictly increasing in the open interval $t\in(0,1)$, for all dimensions D.*

Proof. We prove this by showing that the first derivative of the $C_G(t)$ with respect to t is strictly positive. First note that since $C_G(t)>0$ is a positive function in the interval $t\in(0,1)$. This means showing $\frac{\mathrm{d}}{\mathrm{d}t}C_G(t)>0$ is equivalent to showing that $\frac{\mathrm{d}}{\mathrm{d}t}\log C_G(t)>0$. The derivative of the logarithm of (7.41) is

$$\frac{\mathrm{d}}{\mathrm{d}t}\log C_G(t) = \frac{2\pi}{D^2}\sum_{r=1}^{D-1}r(D-r)\cot(\pi rt/D), \tag{7.42}$$

where $\cot(\cdot)$ denotes the cotangent function. We differentiate again to get

$$\frac{\mathrm{d}^2}{\mathrm{d}t^2}\log C_G(t) = -\frac{2\pi^2}{D^3}\sum_{r=1}^{D-1}r^2(D-r)\frac{1}{\sin^2(\pi rt/D)}. \tag{7.43}$$

Note that the right hand side of (7.43) is strictly negative whenever $t>0$, which implies that the first derivative of the logarithm (7.42) is a strictly decreasing function of t and hence achieving its minimum value at $t=1$, which is given by

$$\frac{\mathrm{d}}{\mathrm{d}t}\log C_G(t)\,|_{t=1} = \frac{2\pi}{D^2}\sum_{r=1}^{D-1}r(D-r)\cot(\pi r/D) = 0, \tag{7.44}$$

where the last equality follows from symmetry considerations (terms cancel one by one). We have shown $\frac{\mathrm{d}}{\mathrm{d}t}\log C_G(t)>0 \Leftrightarrow \frac{\mathrm{d}}{\mathrm{d}t}C_G(t)>0$ and therefore we conclude that the G-concurrence is strictly increasing for $t\in(0,1)$. □

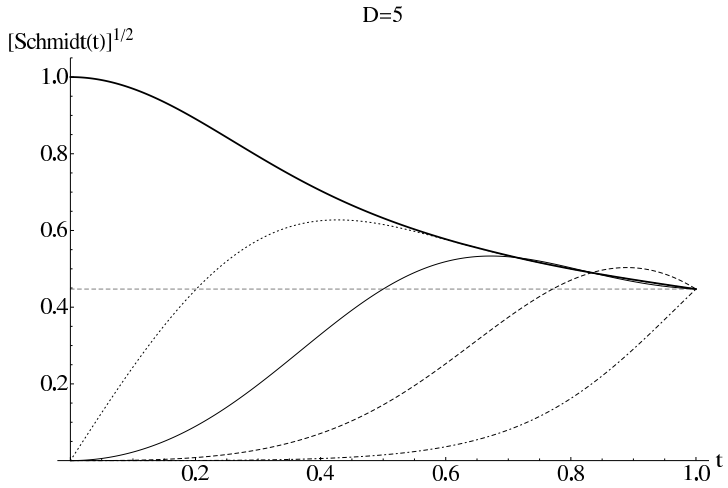

Figure 7.5: The square roots of the Schmidt coefficients as functions of t for $D = 5$. Note how at $t = 0$ all coefficients but one are zero, and how at $t = 1$ all coefficients are equal in magnitude to $1/\sqrt{5}$, with a continuous variation in between. The dashed line represents the $1/\sqrt{5}$ constant function.

7.3.2 Extension to multipartite systems

The construction presented in Theorem 7.3 can be easily generalized to multipartite systems of arbitrary dimension. The concept of maximally entangled states is not defined for three parties or more, so in this case, the family continuously interpolates between a product basis and a qudit graph basis. It is still true that for a fixed t, all basis states constructed this way have the same entanglement (as quantified by any entanglement measure) since they only differ by local unitaries.

As a specific example, consider the tripartite GHZ state $(|000\rangle + |111\rangle)/\sqrt{2}$. This state is a stabilizer state [NC00] and therefore is local-unitary equivalent [Schb] to a graph state $|G\rangle = (C_{12}C_{23}C_{13})|+\rangle_1|+\rangle_2|+\rangle_3$, where the subscripts on C indicates which pair of qubits the C gate is applied to. By varying the "strength" of the controlled-Phase gate, one can now construct a family of equally entangled basis for the Hilbert space of 3 qubits that continuously interpolates between a product basis and the GHZ-like graph basis. This GHZ construction can be easily generalized to higher dimensions and also to n parties by using the complete graph given by

$$|G_{\mathrm{GHZ}}(t)\rangle := \prod_{i=1}^{n-1}\prod_{j>i}^{n} C_{ij}(t)\ |+\rangle^{\otimes n} \tag{7.45}$$

where $|+\rangle$ is defined in (7.20) and $C(t)$ is defined in (7.28). Finally note that this construction works for any graph state of any dimension, and not just for GHZ-like graph states. Such bases with tunable entanglement may be of use in the study of multipartite entanglement.

7.3.3 Examples

In this subsection we perform a similar analysis as the one in Sec. 7.2.4, so that one can easily compare the behaviour of both solutions.

We consider again a $D = 5$ example, for which we plot in Fig. 7.5 the square root of the Schmidt coefficients as functions of t. It is easy to see that indeed the basis interpolates between a product basis and a maximally entangled one in a continuous manner. As proven in Lemma 7.4, all Schmidt coefficients are non-zero for $t > 0$.

In Fig. 7.6 we plot the same quantities for $D = 8$.

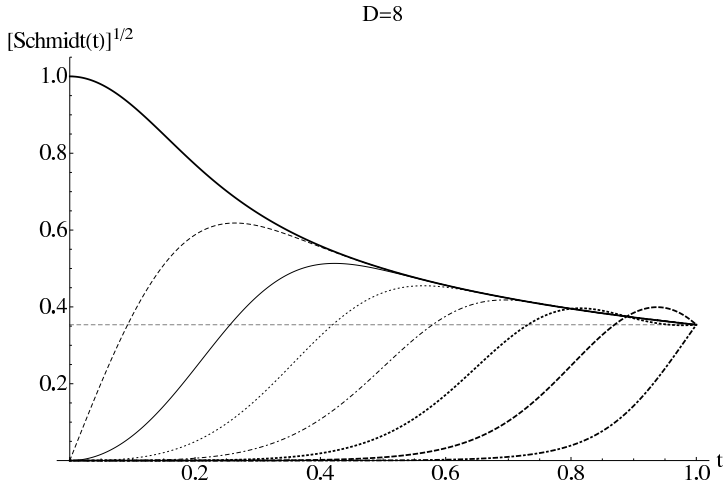

Figure 7.6: The square roots of the Schmidt coefficients as functions of t for $D = 8$. Again note how at $t = 0$ all coefficients but one are zero, and how at $t = 1$ all coefficients are equal in magnitude to $1/\sqrt{8}$, with a continuous variation in between. The dashed line represents the $1/\sqrt{8}$ constant function.

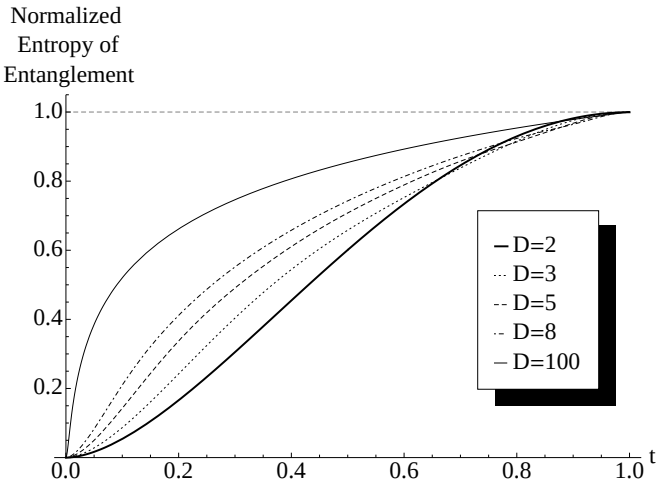

Figure 7.7: The entropy of entanglement as function of t for various dimensions. Note that the variation seems to be monotonically increasing for all D, a statement we did not prove.

Observe how in both examples above the variation of the Schmidt coefficients is not oscillatory, as in the examples of Sec. 7.2.4.

In Fig. 7.7 we plot the entropy of entanglement of the basis states as a function of t for dimensions $D = 2, 3, 5, 8$ and 100. We observe that the entropy of entanglement varies continuously and monotonically between 0 and 1. It is not known if the entropy of entanglement is always strictly increasing for all D although we verified this by visual inspection for all $D \leqslant 10$. In Fig. 7.8, we

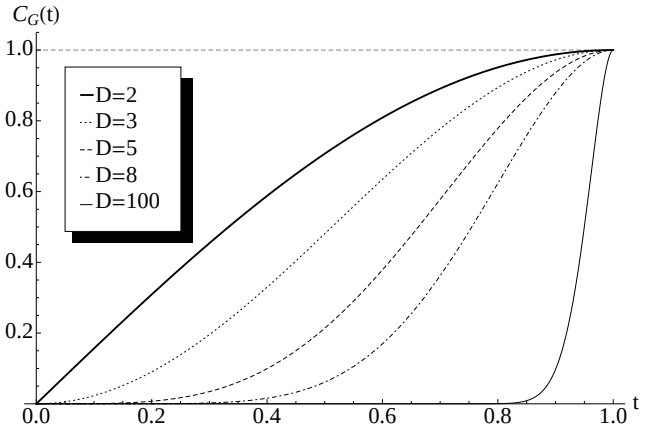

Figure 7.8: The G-concurrence as function of t for various dimensions. The variation is strictly increasing in t for all D as shown in Lemma 7.6.

plot the G-concurrence for the same dimensions. We see how the curves are strictly increasing and this is true for all D as proven in Lemma 7.6.

7.4 Conclusion

We have solved the problem posed in [KM06] by providing two families of equientangled bases for two identical qudits for arbitrary dimension D. The construction of the first solution is based on quadratic Gauss sums and follows along the lines of [KM06], whereas the second family is constructed using a different method based on qudit graph states.

The first solution based on quadratic Gauss sums has an explicit analytic expression for the Schmidt coefficients that is easy to evaluate since they are just sums with D terms (see (7.13) and (7.14)). However some Schmidt coefficients can be zero and the entropy of entanglement of the states in the basis varies non-monotonically with t for $D > 2$.

The second solution based on graph states consists entirely of full Schmidt rank states for any $0 < t \leqslant 1$ that seem to have an entropy of entanglement that is strictly increasing as t increases. Unfortunately we did not find a simple analytic expression for the Schmidt coefficients, but they can be computed numerically without much difficulty. We found a simple analytic expression for another pure state entanglement measure, the G-concurrence, which we proved is strictly increasing as t increases. Finally we remark that one can extend this construction to equally entangled bases of more than two parties that interpolate continuously between a product basis and a graph basis even if the concept of maximally entangled states is not defined for more than two parties. This construction may be of interest in studying multipartite entanglement.

Bibliography

[ACP04] Fabio Anselmi, Anthony Chefles, and Martin B. Plenio. Local copying of orthogonal entangled quantum states. *New J. Phys.*, 6:164, 2004.

[AK01] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inf. Theory*, 47:3065–3072, 2001.

[AKP] V. Arvind, Piyush P. Kurur, and K. R. Parthasarathy. Non-stabilizer quantum codes from abelian subgroups of the error group. e-print arXiv:quant-ph/0210097.

[BB] Mohsen Bahramgiri and Salman Beigi. Graph states under the action of local clifford group in non-binary case. arXiv:quant-ph/0610267.

[BBC+93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William Kent Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 1993.

[BBP+96] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76(5):722–725, 1996.

[BDF+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William Kent Wootters. Quantum nonlocality without entanglement. *Phys. Rev. A*, 59(2):1070–1091, 1999.

[BE81] Bruce C. Berndt and Ronald J. Evans. The determination of gauss sums. *Bull. Am. Math. Soc. New Ser*, 5:107–129, 1981.

[Bén] Cédric Bény. Conditions for the approximate correction of algebras. e-print arXiv:0907.4207 [quant-ph].

[Bha97] Rajendra Bhatia. *Matrix Analysis*. Springer-Verlag, New York, 1997.

[BKK07a] Cédric Bény, Achim Kempf, and David W. Kribs. Generalization of quantum error correction via the heisenberg picture. *Phys. Rev. Lett.*, 98(10):100502, 2007.

[BKK07b] Cédric Bény, Achim Kempf, and David W. Kribs. Quantum error correction of observables. *Phys. Rev. A*, 76(4):042303, 2007.

[BKNPV08] Robin Blume-Kohout, Hui Khoon Ng, David Poulin, and Lorenza Viola. Characterizing the structure of preserved information in quantum processes. *Phys. Rev. Lett.*, 100(3):030501, 2008.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69(20):2881–2884, Nov 1992.

[BZ06] Ingemar Bengtsson and Karol Życzkowski. *Geometry of Quantum States*. Cambridge University Press, Cambridge, 2006.

[CKK+07] Sujit K. Choudhary, Guruprasad Kar, Samir Kunkri, Ramij Rahaman, and Anirban Roy. Local cloning of genuinely entangled states of three qubits. *Phys. Rev. A*, 76(6):062312, 2007.

[CKRR07] Sujit K. Choudhary, Samir Kunkri, Ramij Rahaman, and Anirban Roy. Local cloning of entangled qubits. *Phys. Rev. A*, 76(5):052305, 2007.

[Coh07] Scott M. Cohen. Local distinguishability with preservation of entanglement. *Phys. Rev. A*, 75(5):052313, 2007.

[CP90] Randy Carraghan and Panos M. Pardalos. An exact algorithm for the maximum clique problem. *Operations Research Letters*, 9(6):375–382, 1990.

[CRSS98] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory*, 44:1369–1387, 1998. arXiv:quant-ph/9608006.

[CS96] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098–1105, 1996.

[CSSZ09] Andrew Cross, Graeme Smith, John A. Smolin, and Bei Zeng. Codeword stabilized quantum codes. *IEEE Trans. Inf. Theory*, 55(1):433, 2009.

[CT05] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, New York, 2nd edition edition, 2005.

[CW87] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. In *STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 1–6, New York, NY, USA, 1987. ACM.

[CZC08] Xie Chen, Bei Zeng, and Isaac L. Chuang. Nonbinary codeword-stabilized quantum codes. *Phys. Rev. A*, 78(6):062315, Dec 2008.

[DFY] Runyao Duan, Yuan Feng, and Mingsheng Ying. Distinguishability of quantum states by separable operations. e-print arXiv:0705.0795 [quant-ph].

[EW05] Graham Everest and Thomas Ward. *An Introduction to Number Theory*. Springer-Verlag (Graduate Texts in Mathematics), 2005.

[Fey82] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, June 1982.

[GBP97] M. Grassl, Th. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56(1):33–38, 1997.

[GBR04] Markus Grassl, Thomas Beth, and Martin Roetteler. On optimal quantum codes. *Int. J. Quantum Inf.*, 2:55–64, 2004.

[GG07] Vlad Gheorghiu and Robert B. Griffiths. Entanglement transformations using separable operations. *Phys. Rev. A*, 76(3):032310, 2007.

[GG08] Vlad Gheorghiu and Robert B. Griffiths. Separable operations on pure states. *Phys. Rev. A*, 78(2):020304, 2008.

[GJ79] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman, 1979.

[GKR] Markus Grassl, Andreas Klappenecker, and Martin Roetteler. Graphs, quadratic forms and quantum codes. e-print arXiv:quant-ph/0703112.

[GKR04] Sibasish Ghosh, Guruprasad Kar, and Anirban Roy. Local cloning of bell states and distillable entanglement. *Phys. Rev. A*, 69(5):052312, 2004.

[GL] Vlad Gheorghiu and Shiang Yong Looi. Construction of Equientangled Bases in Arbitrary Dimensions via Quadratic Gauss Sums and Graph States. e-print arXiv:1004.1633 [quant-ph].

[GLG10] Vlad Gheorghiu, Shiang Yong Looi, and Robert B. Griffiths. Location of quantum information in additive graph codes. *Phys. Rev. A*, 81(3):032326, 2010.

[Gota] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. e-print arXiv:quant-ph/9802007.

[Gotb] Daniel Gottesman. Stabilizer codes and quantum error correction. e-print arXiv:quant-ph/9705052.

[Gou05] Gilad Gour. Family of concurrence monotones and its applications. *Phys. Rev. A*, 71(1):012318, 2005.

[Gra07] Markus Grassl. Bounds on the minimum distance of linear codes. Online available at http://www.codetables.de, 2007.

[Gri96] Robert B. Griffiths. Consistent histories and quantum reasoning. *Phys. Rev. A*, 54(4):2759–2774, 1996.

[Gri02] Robert B. Griffiths. *Consistent Quantum Theory*. Cambridge University Press, Cambridge, 2002.

[Gri05] Robert B. Griffiths. Channel kets, entangled states, and the location of quantum information. *Phys. Rev. A*, 71(4):042337, 2005.

[Gri07] Robert B. Griffiths. Types of quantum information. *Phys. Rev. A*, 76(6):062320, 2007.

[GWYC06] Robert B. Griffiths, Shengjun Wu, Li Yu, and Scott M. Cohen. Atemporal diagrams for quantum circuits. *Phys. Rev. A*, 73(5):052309, 2006.

[GYC] Vlad Gheorghiu, Li Yu, and Scott M. Cohen. Local cloning of entangled states. e-print arXiv:1004.5126 [quant-ph].

[Ham89] Morton Hamermesh. *Group Theory and its Application to Physical Problems*. Dover Publications, Inc, 1989.

[HDE+] M. Hein, W. Dur, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in graph states and its applications. e-print arXiv:quant-ph/0602096.

[HDM05] Erik Hostens, Jeroen Dehaene, and Bart De Moor. Stabilizer states and clifford operations for systems of arbitrary dimensions and modular arithmetic. *Phys. Rev. A*, 71(4):042315, 2005.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865–942, Jun 2009.

[HJ99] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 1999.

[HLP99] G. H. Hardy, J. E. Littlewood, and G. Pólya. *Inequalities*. Cambridge University Press, 1999.

[HTZ+08] Dan Hu, Weidong Tang, Meisheng Zhao, Qing Chen, Sixia Yu, and C. H. Oh. Graphical nonbinary quantum error-correcting codes. *Phys. Rev. A*, 78(1):012306, 2008.

[HW08] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford University Press, New York, 8th edition, 2008.

[IM07] Lev Ioffe and Marc Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75(3):032345, 2007.

[JP99] Daniel Jonathan and Martin B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Phys. Rev. Lett.*, 83(7):1455–1458, 1999.

[Kay06] Alastair Kay. Private communication, 2006.

[KE06] Alastair Kay and Marie Ericsson. Local cloning of arbitrarily entangled multipartite states. *Phys. Rev. A*, 73(1):012343, 2006.

[KKKS06] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeeep Kiran Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory*, 51:4892–4913, 2006.

[KL97] Emanuel Knill and Raymond Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(2):900–911, 1997.

[KM06] V. Karimipour and L. Memarzadeh. Equientangled bases in arbitrary dimensions. *Phys. Rev. A*, 73(1):012329, 2006.

[LMPZ96] Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek. Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77(1):198–201, 1996.

[LP01] Hoi-Kwong Lo and Sandu Popescu. Concentrating entanglement by local actions: beyond mean values. *Phys. Rev. A*, 63(2):022301, 2001.

[LYGG08] Shiang Yong Looi, Li Yu, Vlad Gheorghiu, and Robert B. Griffiths. Quantum-error-correcting codes using qudit graph states. *Phys. Rev. A*, 78(4):042303, 2008.

[Ma07] Zhong-Qi Ma. *Group Theory for Physicists*. World Scientific Publishing Co. Pte. Ltd., Singapore, 2007.

[Mic95] Hazewinkel Michiel. *Encyclopaedia of Mathematics: Regular Representation. Online available at http://eom.springer.de/*. Kluwer Academic Publishers, The Netherlands, 1995.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, Amsterdam, 1977.

[MS08] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78(4):042309, 2008.

[Nat00] Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Springer-Verlag (Graduate Texts in Mathematics), 2000.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 5th edition, 2000.

[New72] Morris Newman. *Integral Matrices*. Academic Press, New York, 1972.

[Nie] Michael A. Nielsen. Majorization and its applications to quantum information theory. Unpublished lecture notes of a course given at Caltech, Pasadena.

[Nie99] Michael A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2):436–439, 1999.

[OH06] Masaki Owari and Masahito Hayashi. Local copying and local discrimination as a study for nonlocality of a set of states. *Phys. Rev. A*, 74(3):032108, 2006.

[Rai99] Eric M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory*, 45(6):1827–1832, 1999.

[RB01] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, 2001.

[RHSS97] Eric M. Rains, R. H. Hardin, Peter W. Shor, and N. J. A. Sloane. A nonadditive quantum code. *Phys. Rev. Lett.*, 79(5):953–954, Aug 1997.

[Scha] Dirk Schlingemann. Logical network implementation for cluster states and graph codes. e-print arXiv:quant-ph/0202007.

[Schb] Dirk Schlingemann. Stabilizer codes can be realized as graph codes. e-print arXiv:quant-ph/0111080.

[Sch95] Benjamin Schumacher. Quantum coding. *Phys. Rev. A*, 51(4):2738–2747, 1995.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell system technical journal*, 27, 1948.

[Sho95] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):R2493–R2496, 1995.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[SIGA05] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Rev. Mod. Phys.*, 77(4):1225–1256, Nov 2005.

[SSW07] John A. Smolin, Graeme Smith, and Stephanie Wehner. Simple family of nonadditive quantum codes. *Phys. Rev. Lett.*, 99(13):130505, Sep 2007.

[Ste96] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5):793–797, Jul 1996.

[Sto96] Arne Storjohann. Near optimal algorithms for computing smith normal forms of integer matrices. In *ISSAC '96: Proceedings of the 1996 international symposium on Symbolic and algebraic computation*, pages 267–274, New York, NY, USA, 1996. ACM.

[SW01] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65(1):012308, 2001.

[Tur37] A. M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proc. London Math. Soc.*, s2-42(1):230–265, 1937.

[Vid99] Guifré Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.*, 83(5):1046–1049, 1999.

[WSHV00] Jonathan Walgate, Anthony J. Short, Lucien Hardy, and Vlatko Vedral. Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.*, 85(23):4972–4975, Dec 2000.

[WZ82] William Kent Wootters and Wojciech Hubert Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[YCLO08] Sixia Yu, Qing Chen, C. H. Lai, and C. H. Oh. Nonadditive quantum error-correcting code. *Phys. Rev. Lett.*, 101(9):090501, Aug 2008.

[YCO] Sixia Yu, Qing Chen, and C.H. Oh. Graphical quantum error-correcting codes. e-print arXiv:0709.1780 [quant-ph].

[YGC10] Li Yu, Robert B. Griffiths, and Scott M. Cohen. Efficient implementation of bipartite nonlocal unitary gates using prior entanglement and classical communication. *Phys. Rev. A*, 81(6):062315, Jun 2010.

[ZB04] Karol Życzkowski and Ingemar Bengtsson. On duality between quantum maps and quantum states. *Open Syst. Inf. Dyn.*, 11:3–42, 2004.